



**Technical Reference Guide,
Open Terminal Requirement
Specification - Book 1**

**Functional Implementation
2013-11-15**

VERSION 3.3.4

This page is intentionally left blank

How to Contact Nets Denmark A/S

Contact addresses are found on www.nets.eu

Disclaimers

Copyright Information

This document contains information proprietary to Nets Denmark A/S. The information, whether in the form of e.g. text, schematics, tables, drawings or illustrations, must not, without the prior, written consent of Nets Denmark A/S, be copied, reproduced or otherwise duplicated, disclosed outside the recipient company or organization or used by the recipient for purposes other than those explicitly agreed in writing with Nets Denmark A/S.

This limitation does not limit the recipient's right to duplicate and use information contained in the document if such information is received from another source without restriction provided such source is not in breach of an obligation of confidentiality towards Nets Denmark A/S.

Trademarks

Nets and the Nets-logo are registered trademarks of Nets Denmark A/S. Dankort, VISA, Eurocard, MasterCard and Maestro names and logos are registered trademarks of Nets Denmark A/S and its international partners.

Limitation of Liability

Under no circumstances shall Nets Denmark A/S be liable for any direct incidental, indirect, special or consequential damages whatsoever (including but not limited to lost profits) arising out of or relating to this document or the information contained in it, even if Nets Denmark A/S has been advised, knew or should have known of the possibility of such damages.

Disputes

Any disputes arising from information contained in this document or work relating hereto will be settled in the Danish courts in accordance with Danish law.

Certification

Any new or updated type of Terminal must be certified by Nets Denmark A/S before being installed at Merchant locations and being prepared for transmission of transactions to Nets Denmark A/S.

This page is intentionally left blank

1-1 Table of Contents

Technical Reference Guide, Open Terminal Requirement Specification - Book 1	i
1-1 Table of Contents	1-1-1
1-2 Revision Log, Book 1	1-2-1
1-3 Introduction	1-3-1
1-3.1 Overview	1-3-1
1-3.1.1 Audience	1-3-1
1-3.1.2 Prerequisites	1-3-1
1-3.1.3 Scope	1-3-1
1-3.2 Target Group	1-3-1
1-3.3 Objectives	1-3-2
1-3.4 Level of Detail	1-3-2
1-3.5 Document Structure	1-3-3
1-4 Definitions	1-4-1
1-4.1 Introduction	1-4-1
1-4.2 Terminology	1-4-1
1-4.2.1 Abbreviations	1-4-1
1-4.2.2 Terms	1-4-4
1-4.2.3 Notation	1-4-5
1-4.3 Requirement Numbering	1-4-7
1-4.4 References	1-4-8
1-4.5 Bibliography	1-4-12
1-4.6 Related Websites	1-4-13
1-5 System Overview	1-5-1
1-5.1 Introduction	1-5-1
1-5.2 Standards	1-5-1
1-5.3 Business Requirements	1-5-3
1-5.3.1 Payment Services	1-5-3
1-5.3.2 Acceptance Technologies	1-5-4
1-5.3.3 Acceptance Environments	1-5-4
1-5.3.4 Cardholder Verification Methods	1-5-5
1-5.3.5 Card Authentication Methods	1-5-5
1-5.3.6 Functions	1-5-5
1-5.3.7 Terminal Types	1-5-6
1-5.4 Certification of Terminals	1-5-6
1-6 Terminal Types and Environments	1-6-1
1-6.1 Terminal Types	1-6-1
1-6.1.1 Terminal Environments, Debit/Credit	1-6-2
1-6.1.2 Cardholder Verification Methods	1-6-4
1-6.2 Cash/Quasi-Cash Terminals	1-6-4
1-6.3 POS Terminal/UPT Levels vs. Terminal Type	1-6-5

1-7 Payment Card Industry - Data Security Standard	1-7-1
1-7.1 PCI - DSS	1-7-1
1-7.1.1 Priority of PCI SSC Standards	1-7-1
1-7.1.2 Centralized log handling	1-7-1
1-7.1.3 Receipts and Truncation of the PAN	1-7-3
1-7.1.4 Transaction Log	1-7-3
1-7.1.5 Tools for transaction follow-up	1-7-4
1-7.1.6 Handling of PAN in Merchant Application	1-7-4
1-7.1.7 Handling of Track2 Data	1-7-5
1-7.1.8 Handling of Key Entered card data	1-7-5
1-7.1.9 Use of derived identification	1-7-6
1-7.2 Nets PA-DSS Implementation Guide	1-7-6
1-8 Basic Transaction Flow	1-8-1
1-8.1 The Four Steps	1-8-1
1-8.1.1 Introduction	1-8-1
1-8.1.2 The Basic Commands	1-8-1
1-9 Best Practice	1-9-1
1-9.1 Introduction	1-9-1
1-9.2 Documentation	1-9-1
1-9.3 Terminal Categories	1-9-1
1-9.4 Choice of Business Call	1-9-2
1-9.5 Support of Card Technologies	1-9-3
1-9.6 ICC Technology and Fallback to Magnetic Stripe	1-9-3
1-9.7 Service Packs	1-9-3
1-9.8 Application Selection	1-9-4
1-9.9 Support of Cardholder Verification Methods	1-9-4
1-9.10 Temporary Offline Procedure	1-9-5
1-9.11 Voice Authorization Calls	1-9-6
1-9.12 Stop List	1-9-7
1-9.13 Optimizing the Transaction Time	1-9-8
1-9.13.1 Parallel Processing	1-9-8
1-9.13.2 Start before amount is known	1-9-8
1-9.13.3 Data Transmission	1-9-9
1-9.14 Signature Verification and Accept	1-9-10
1-9.15 Receipts	1-9-10
1-9.16 Transaction Result	1-9-11
1-9.17 Transaction Checks	1-9-12
1-9.18 Cashback Amount	1-9-13
1-9.19 Addition of Surcharges and Fees	1-9-13
1-9.20 Gratuity	1-9-13
1-9.21 Dual Communication Access Points	1-9-14
1-9.22 Balancing and the Transfer of Advices	1-9-15
1-9.23 Log and Totals	1-9-15
1-9.24 Merchant Application Log	1-9-16
1-9.25 Guidelines for Constructing Total Reports	1-9-16
1-9.25.1 Introduction	1-9-16
1-9.25.2 General	1-9-16

1-9.25.3	Data Elements	1-9-17
1-9.25.4	Example	1-9-18
1-9.25.5	Proposal for accumulating data for Totalling Reports	1-9-20
1-9.25.6	Total Reports and DCC	1-9-25
1-9.26	Host Messages	1-9-26
1-9.27	Transaction State Information	1-9-26
1-9.28	Local PIN	1-9-26
1-9.29	Placement and Installation of terminal	1-9-27
1-9.29.1	Mounting of the PIN Entry Device in the terminal ...	1-9-27
1-9.29.2	Placement of the terminal	1-9-27
1-10	Functionalities	1-10-1
1-10.1	Introduction	1-10-1
1-10.2	Business Calls to the PSAM	1-10-2
1-10.2.1	Purchase	1-10-2
1-10.2.2	Original Authorization	1-10-2
1-10.2.3	Extended Authorization	1-10-3
1-10.2.4	Supplementary Authorization	1-10-5
1-10.2.5	Capture	1-10-6
1-10.2.6	Refund	1-10-6
1-10.2.7	Authorization Reversal	1-10-7
1-10.2.8	Cancellation	1-10-7
1-10.3	Cash	1-10-10
1-10.4	Private Label Card Scheme Recognition	1-10-11
1-10.5	Terminal Services	1-10-11
1-10.5.1	Additional Card BIN Information	1-10-11
1-10.5.2	Additional Transaction Information	1-10-12
1-10.5.3	Account Type Selection	1-10-15
1-10.5.4	Cashback	1-10-16
1-10.5.5	VAT	1-10-16
1-10.5.6	Payment Condition Code	1-10-17
1-10.5.7	Post Registration	1-10-17
1-10.5.8	Acquirer Information	1-10-18
1-10.5.9	Selectable Kernel Configurations	1-10-19
1-10.5.10	Preferred Offline processing	1-10-21
1-10.5.11	Forced processing	1-10-21
1-10.6	Processing Condition Table	1-10-22
1-10.6.1	Introduction	1-10-22
1-10.6.2	Data handling	1-10-22
1-10.6.3	Processing	1-10-23
1-10.6.4	Processing conditions controlled by the PCT	1-10-25
1-10.6.5	Data Objects	1-10-26
1-10.7	Special Status Services	1-10-28
1-10.7.1	Duplicate Transaction Check by the PSAM	1-10-28
1-10.7.2	Status of Previous Transaction	1-10-28
1-10.7.3	The Get Debit/Credit Properties Command	1-10-29
1-10.7.4	Purpose of this Functionality	1-10-29
1-10.7.5	Limitations	1-10-31
1-10.8	Contactless Transactions	1-10-33
1-10.8.1	Introduction	1-10-33
1-10.8.2	Kernel Configuration	1-10-33
1-10.8.3	Contactless Transactions	1-10-34
1-10.8.4	Transaction Flow - External Kernel	1-10-34

1-10.8.5	Rejected/Declined Transactions	1-10-40
1-10.8.6	Protection against Replay Attacks	1-10-42
1-10.8.7	CVM Handling	1-10-42
1-10.8.8	Contactless Limits	1-10-43
1-10.8.9	Application Program ID	1-10-44
1-10.8.10	Restrictions for Contactless Transaction	1-10-44
1-10.8.11	Optional Functions	1-10-45
1-10.9	Prepaid MSC Transactions	1-10-46
1-10.9.1	Functional Requirements	1-10-46
1-10.9.2	Host Data Transfer	1-10-47
1-10.9.3	Prepaid MSC Transaction Flow	1-10-48
1-10.9.4	Error Situations	1-10-49
1-10.9.5	Entry of PAN Information	1-10-50
1-10.10	Loyalty information	1-10-52
1-10.10.1	Introduction	1-10-52
1-10.10.2	Using MSC cards	1-10-52
1-10.10.3	Using ICC cards	1-10-53
1-10.10.4	Expiration Date	1-10-54
1-10.10.5	Masking of data	1-10-54
1-10.10.6	Dual Card Reference	1-10-56
1-10.11	Token transactions	1-10-57
1-10.11.1	Introduction	1-10-57
1-10.11.2	General requirements	1-10-57
1-10.11.3	Flow of information	1-10-58
1-10.11.4	Token based Transaction Types	1-10-59
1-10.11.5	Token - Contents and Identification Keys	1-10-61
1-10.11.6	Token and Cardholder verification method	1-10-63
1-10.11.7	Token Management Functions	1-10-64
1-10.12	Token Macro Functions	1-10-65
1-10.12.1	Macro MAKE PURCHASE	1-10-66
1-10.12.2	Macro AUTHORIZE	1-10-66
1-10.12.3	Macro AUTHORIZATION ADD	1-10-68
1-10.12.4	Macro FINALIZE	1-10-69
1-10.12.5	Macro RELEASE	1-10-72
1-10.12.6	Macro MAKE REFUND	1-10-72
1-10.12.7	Macro AUTHORIZE FOR TIPS	1-10-73
1-10.12.8	Macro FINALIZE WITH TIPS	1-10-75
1-10.13	Special Functions	1-10-78
1-10.13.1	Special Functions - Hotels	1-10-78
1-10.13.2	Merchant Functions - Restaurant	1-10-80
1-10.13.3	Merchant Functions - Car Rental	1-10-80
1-10.13.4	Token and Unattended Payment Terminals	1-10-80
1-10.14	DCC - Dynamic Currency Conversion	1-10-81
1-10.14.1	Introduction	1-10-81
1-10.14.2	Getting the DCC pre-information	1-10-83
1-10.14.3	DCC-Transaction-Information	1-10-87
1-10.14.4	Transfer of DCC-Trans.-Info to the PSAM	1-10-88
1-10.14.5	DCC currency conversion formulas	1-10-90
1-10.14.6	Transaction log	1-10-92
1-10.14.7	DCC Selection of Currency	1-10-93
1-10.14.8	DCC transaction types	1-10-95
1-10.14.9	DCC receipt types	1-10-96

1-10.15	Transactions with Tips/Gratuity	1-10-96
1-10.15.1	Introduction	1-10-96
1-10.15.2	Method 1, Tips on invoice	1-10-97
1-10.15.3	Method 2, Tips on pre-receipt	1-10-97
1-10.15.4	Method 3, Tips on display	1-10-98
1-10.15.5	Method 4, Tips on receipt	1-10-102
1-10.15.6	Method 5, Tips before the card is known	1-10-104
1-11	Display Texts	1-11-1
1-11.1	Introduction	1-11-1
1-11.1.1	Language Requirements	1-11-1
1-11.1.2	Combined Approval of Amount and PIN	1-11-2
1-11.2	Messages for Display	1-11-2
1-11.3	Display flow for Transactions	1-11-7
1-11.3.1	Example 1: Display flow PIN Trans. - Approved	1-11-7
1-11.3.2	Example 2: Display flow PIN Trans. - PIN Error	1-11-8
1-11.3.3	Example 3: Display flow PIN Trans. - PIN Retry	1-11-9
1-11.3.4	Example 4: Display flow Signature Trans. - Approved	1-11-11
1-11.3.5	Example 5: Display flow Signature Trans. - Approved	1-11-12
1-11.4	Display flow for Transactions - max. 16 Char. per Line	1-11-13
1-11.4.1	Example 1: Display flow PIN Trans. - Approved	1-11-13
1-11.4.2	Example 2: Display flow PIN Trans. - PIN Error	1-11-14
1-11.4.3	Example 3: Display flow PIN Trans. - PIN Retry	1-11-15
1-11.4.4	Example 4: Display flow Signature Trans. - Approved	1-11-17
1-11.4.5	Example 5: Display flow Signature Trans. - Approved	1-11-17
1-11.5	PIN Entry flow	1-11-18
1-11.5.1	Requirements for PIN Entry State	1-11-18
1-11.6	Terms - Business Calls and Admin. Functions	1-11-20
1-11.6.1	Introduction	1-11-20
1-11.6.2	Business Calls	1-11-21
1-11.6.3	Administrative Functions	1-11-22
1-12	Receipts	1-12-1
1-12.1	Functional requirements	1-12-1
1-12.1.1	Generic	1-12-1
1-12.1.2	Special Considerations for Unattended Terminals	1-12-3
1-12.1.3	Automated Fuel Dispensers	1-12-4
1-12.1.4	DCC Functional Requirement	1-12-5
1-12.2	Standard Receipt Layout	1-12-6
1-12.2.1	Receipt Language	1-12-6
1-12.2.2	Emphasizing of Text	1-12-6
1-12.2.3	Generic Layout	1-12-7
1-12.2.4	Receipt Header	1-12-8
1-12.2.5	Merchant Information	1-12-8
1-12.2.6	Header Information	1-12-9
1-12.2.7	Amount Information	1-12-10
1-12.2.8	Transaction Information	1-12-13
1-12.2.9	Signature Information	1-12-19
1-12.2.10	Footer Information	1-12-21
1-12.2.11	Prepaid Card Information	1-12-24
1-12.2.12	Receipt Footer	1-12-25
1-12.2.13	Pre - receipt	1-12-25
1-12.3	DCC Receipt Layout	1-12-25
1-12.3.1	Receipt Language	1-12-26

1-12.3.2	Pre-receipt Structure	1-12-26
1-12.3.3	Generic DCC Receipt Structure	1-12-29
1-12.3.4	Compiled DCC Receipt Information	1-12-36
1-12.4	Examples of Receipts (Informative)	1-12-38
1-12.4.1	A - Full Template	1-12-42
1-12.4.2	B - Basic PIN Transaction, ICC.	1-12-45
1-12.4.3	C - Extended PIN (Copy of Receipt) MSC	1-12-46
1-12.4.4	D - PIN, ICC Fallback to MSC	1-12-47
1-12.4.5	E - Signature, Merchant, VAT	1-12-48
1-12.4.6	F - Signature, Cardholder, VAT	1-12-49
1-12.4.7	G - Refund	1-12-50
1-12.4.8	H - Cancellation	1-12-51
1-12.4.9	I - Original Authorization, Key Entered	1-12-52
1-12.4.10	J - Original Authoriz, ICC, PIN, Cardholder	1-12-53
1-12.4.11	K - Supplementary Authorization	1-12-54
1-12.4.12	L - Reversal of Authorization	1-12-55
1-12.4.13	M - Capture, No CVM, Signature, Merchant	1-12-56
1-12.4.14	N - Capture, PIN, Signature, Cardholder	1-12-57
1-12.4.15	O - Cash, Signature	1-12-58
1-12.4.16	P - Post Registration	1-12-59
1-12.4.17	Q - Failed Transaction	1-12-60
1-12.4.18	R - Interrupted Transaction	1-12-61
1-12.4.19	S - Declined Transaction	1-12-62
1-12.4.20	T - Signature Declined	1-12-63
1-12.4.21	AA - Prepaid MSC, Purch. with Cashback	1-12-64
1-12.4.22	AB - Prepaid MSC, Load	1-12-65
1-12.4.23	AC - Prepaid MSC, Balance	1-12-66
1-12.4.24	AD - Prepaid MSC, Offline Purch. with Cashback	1-12-67
1-12.4.25	BA - Pre-receipt, no Surch./Surch. and Card known .	1-12-68
1-12.4.26	BB - Pre-receipt, Card unknown, Surch.	1-12-69
1-12.4.27	BC - Receipt after On-display Tips, PIN	1-12-70
1-12.4.28	BD - Receipt, Tips after Trans, Merchant	1-12-71
1-12.4.29	BE - Receipt, Tips after Trans, Cardholder's	1-12-72
1-12.4.30	BF - Receipt, Tips after Trans, Cardholder's, Final ...	1-12-73
1-12.4.31	BG - Receipt after Pre-rec. Tips, Sign, Merchant.	1-12-74
1-12.4.32	CA - Pre-receipt, DCC Purchase	1-12-75
1-12.4.33	CB - Pre-receipt, DCC Authorization	1-12-77
1-12.4.34	CC - Pre-receipt, DCC Refund	1-12-78
1-12.4.35	CD - Pre-receipt, DCC Capture	1-12-79
1-12.4.36	CE - DCC, Authorization, Merchant	1-12-80
1-12.4.37	CF - DCC, Authorization, Cardholder	1-12-81
1-12.4.38	CG - DCC, Reversal of Authorization	1-12-82
1-12.4.39	CH - DCC, Capture, Merchant	1-12-83
1-12.4.40	CI - DCC, Capture, Cardholder	1-12-85
1-12.4.41	CJ - DCC, Refund, Cardholder	1-12-87
1-12.4.42	CK - DCC, Purchase, Merchant	1-12-89
1-12.4.43	CM - DCC, Purchase, Cardholder	1-12-91
1-12.4.44	English Receipt Texts	1-12-93
1-13	Single Unit Terminals	1-13-1
1-13.1	Introduction	1-13-1
1-13.2	Conditions and Requirements	1-13-1
1-13.3	Examples	1-13-3

1-14 Business Requirements	1-14-1
1-14.1 General Requirements	1-14-1
1-14.1.1 Business Calls and Terminal Environments	1-14-1
1-14.1.2 Terminal Profiles	1-14-1
1-14.2 Application Initialization	1-14-2
1-14.2.1 Power On	1-14-2
1-14.3 Application Selection	1-14-3
1-14.3.1 Introduction	1-14-3
1-14.3.2 Building the MSC Selection Table	1-14-3
1-14.3.3 Building the AID Selection Table (for ICCs)	1-14-5
1-14.3.4 MSC Application Selection	1-14-11
1-14.3.5 ICC Application Selection	1-14-12
1-14.3.6 Combined MSC and ICC Application Selection	1-14-14
1-14.4 Addendum Records	1-14-16
1-14.4.1 Conditions	1-14-16
1-14.5 Terminal Handlers	1-14-16
1-14.5.1 The Router, Exception Handling	1-14-16
1-14.5.2 The MAD-Handler, Exception Handling	1-14-16
1-14.5.3 The Card Handler, General Requirements	1-14-17
1-14.5.4 User Interface Handler, PIN Pad	1-14-18
1-14.5.5 User Interface Handler, Cardholder Display	1-14-20
1-14.5.6 Merchant App. Handler, Ifc. Term. and Merch. App. ..	1-14-21
1-14.5.7 Data Store Handler, General Requirements	1-14-21
1-14.6 Fallback	1-14-22
1-14.6.1 General Requirements	1-14-22
1-14.7 Cardholder Verification	1-14-22
1-14.7.1 PIN Entry	1-14-22
1-14.7.2 Signature	1-14-22
1-14.8 Protected Functions	1-14-23
1-14.8.1 General Requirements	1-14-23
1-14.8.2 Protected Functions - Manuf. Specific Functions	1-14-23
1-14.9 Reports	1-14-24
1-14.9.1 General Requirements	1-14-24
1-14.10 Log	1-14-24
1-14.10.1 Requirements	1-14-24
1-14.11 Local PIN	1-14-25
1-14.11.1 Business Requirements	1-14-25
1-14.12 Transaction Requirements when using a PSAM	1-14-26
1-14.12.1 Payment, Voice Authorization and Stop List	1-14-26
1-15 Regional Requirements	1-15-1
1-15.1 Introduction	1-15-1
1-15.1.1 Generic Requirements	1-15-2
1-15.1.2 ICC Language Selection	1-15-3
1-15.2 Denmark	1-15-4
1-15.2.1 Danish Regulations	1-15-4
1-15.2.2 Functional Requirements	1-15-5
1-15.2.3 Issuer Information Envelope Data	1-15-5
1-15.2.4 Danish Regional Receipts Requirements	1-15-6
1-15.2.5 Key Legend	1-15-7
1-15.2.6 Display Characters	1-15-8
1-15.2.7 Display Texts	1-15-8
1-15.2.8 Receipt Texts	1-15-13

1-15.3	Sweden	1-15-15
1-15.3.1	Functional Requirements	1-15-15
1-15.3.2	Swedish Regional Receipt Requirements	1-15-18
1-15.3.3	Issuer Information Envelope Data	1-15-19
1-15.3.4	Display Texts	1-15-21
1-15.3.5	Receipt Texts	1-15-26
1-15.4	Norway	1-15-28
1-15.4.1	Functional Requirements	1-15-28
1-15.4.2	Display Texts	1-15-33
1-15.4.3	Receipt Texts	1-15-38
1-15.5	Finland	1-15-41
1-15.5.1	Functional Requirements	1-15-41
1-15.5.2	Display Texts	1-15-41
1-15.5.3	Receipt Texts	1-15-47
1-15.6	Germany	1-15-49
1-15.6.1	Functional Requirements	1-15-49
1-15.6.2	Display Texts	1-15-49
1-15.6.3	Receipt Texts	1-15-54
1-15.7	Poland	1-15-56
1-15.7.1	Functional Requirements	1-15-56
1-15.7.2	Display Texts	1-15-56
1-15.7.3	Receipt texts	1-15-62
1-15.8	Iceland	1-15-63
1-15.8.1	Functional Requirements	1-15-63
1-15.8.2	Display Texts	1-15-63
1-15.8.3	Receipt Texts	1-15-68

1-2 Revision Log, Book 1

Version	Date	Last Page	Affects	Brief Description of Change
1.0	2000-01-17		All pages	Initial production release.
3.0	2009-02-01		All	<p>This Technical Reference Guide has been radically reworked. The original document has been split into two books. All revision descriptions for both books for this initial release of version 3.0 are contained in this chapter</p> <p>Most chapters and sections have updated and improved the descriptions contained therein, e.g. chapter 1-12 page 1-12-1, Receipts.</p> <p>Book one contains general descriptions and general requirements. Functionalities are described on an overall level together with the general matching requirements.</p> <p>Book two contains all the descriptions and requirements for using the functions described in book one together with a PBS/Nets PSAM.</p> <p>The major changes to the specification are:</p> <p>Introduction of Extended Authorization, see section 1-9.4 page 1-9-2 ,Choice of Business Call, section 1-10.2.3 page 1-10-3, Extended Authorization and all sections containing requirements and descriptions for Original Authorizations.</p> <p>A total rewrite of chapter 1-12, Receipts, have been implemented. The reference language is now English. The description of the receipts is divided into different logical blocks with line numbering within the block. Receipts for all types of transactions. A collection of receipt examples is found at the end of the chapter.</p> <p>Introduction of Processing Condition Table, see section 1-10.6 page 1-10-23, Processing Condition Table and section 2-14.5.12 page 2-14-47, Get Processing Condition Table.</p> <p>Introduction of Cancellation, see section 1-10.2.8 page 1-10-7, Cancellation, section 2-4.2.2 page 2-4-3, Cancellation, section 2-5.10 page 2-5-84, Cancellation and section 2-14.7 page 2-14.7, Cancellation</p> <p>Introduction of PCI, see chapter 1-7 page 1-7-1, Payment Card Industry - Data Security Standard.</p> <p>Chapter 1-14, Business Requirements is new. In this section business related (non-technical) requirements have been compiled.</p>

Terminals shall now as a minimum support Service Pack 2. Terminal not supporting any Service Packs or only supporting Service Pack 1 can no longer be approved for production, see section 1-9.7 page 1-9-3, Service Packs.

A new concept for transferring advices from the terminal to the host have been introduced. Exception handling in connection with the transfer of advices have been updated, see section 2-5.15 page 2-5-101, Transferring Advices.

Chapter 1-8, Basic Transaction Flow is all new.

Chapter 1-10.9 Prepaid Card Transactions has been reworked.

In chapter 1-10.11, Token Transactions, chapter 1-10.12, Token Macro Functions and chapter 1-10.13, Merchant Functions the description of the use of Tokens have been reworked.

In chapter 1-10.14, DCC - Dynamic Currency Conversion, the description of the use of DCC have been reworked.

In chapter 1-10.15, Transactions with Tips/Gratuity, the description of the use of tips have been reworked.

Advice Window Size can only have the value 1 or 0, see section 2-5.15.5 page 2-5-107, Advice Window Size.

The number of entries the terminal shall be able to store in the AID Selection Table and the MSC Selection Table have been extended, see section 1-14.3.2 page 1-14-3, Building the MSC Selection Table and section 1-14.3.3 page 1-14-5, Building the AID Selection Table.

The use of tag 'C9' have changed from being an indication to the terminal to perform an Advice Transfer to being an indication to the terminal to perform a PSAM Update, see section 2-5.14.1 page 2-5-98, PSAM Update Flag.

A number of new data elements have been introduced in connection with new functionality, see chapter 2-15 page 2-15-1, Data Elements.

The default language used when defining display texts and receipts is now English.

Display messages in Danish, Swedish, Norwegian, Polish and German are now available. See section 1-15, Regional Require-

				ments.
				Regional/national requirements are now found in chapter 1-15, Regional Requirements
				Chapter 1-5, System Overview and chapter 2-3, System Overview have been reworked.
3.1	2009-07-15	Book 1	Chapter 4	Introduce definition of PCT, Add reference to ISO 4909, EMV Contactless Specification and Visa Transaction Acceptance Device Guide. Add reference to Maestro Best-in-class handling of pre-authorizations.
		Book 1	Chapter 5	Add function Account Type Selection
		Book1	Chapter 10	Rename Prepaid Cards to MSC Prepaid Cards to distinguish it from Contactless (Prepaid) Cards.
				Added notes for the handling of Cancellation w.r.t. requiring confirmation, and not displaying PAN information.
				Clarified the use of Account Type Selection and storage of information in "Envelope".
				Added information on handling "Acquirer Information".
				For token transactions, added information on the use of Card Reference and Extended Authorization and Account Type selection. Note on the use of "Signature on File".Rename terminal macro to token macro. Update figure on Macro AUTHORIZE. Clarification on handling of valid/non-valid token. Update figure on Macro FINALIZE. Update the Macro AUTHORIZE FOR TIPS.
				Adjust amount to use for Card Validation. Note on limits for final amount in captures. Note on token used for tips in restaurants.
		Book 1	Chapter 11	Update display messages to limit size to 16/20 characters.
		Book 1	Chapter 12	Update information on retrieving "Card Name". Inform on the printing of "Acquirer Information".
				Add TCC for Contactless cards. Update on the access to "Reference STAN", available now. Remark to the use of "Clerk ID".
				Specification on printing of "TSI/TVR" information.
				Clarify rules for printing of DCC exchange rates.
				Correct spelling rules in receipt templates.
				Add notes on the origin of TCC in token transactions.

Book 1	Chapter 15	<p>Clarify that Account Type selection may be controlled by PDOL.</p> <p>Add information on "Acquirer Name" printing. Disable requirements for "Post registration".</p> <p>Add information on regional conditions for non-VAT receipts. Add reference to template for Signature Information. Add regional requirement for printing of "TVR/TSI".</p> <p>Add information for regional extended handling of MSC cards. Add information on regional printing of "Acquirer Name".</p> <p>Add information on regional requirements for "TVR/TSI" printing.</p> <p>Add information on regional requirements for <u>truncated</u> PAN printing.</p> <p>Add information on regional reconciliation.</p>
Book 2	Chapter 3	Include handling of MSC track 3.
Book 2	Chapter 4	Include handling of MSC track 3.
Book 2	Chapter 5	Update handling of Advices from MSC pre-paid cards.
Book2	Chapter 12	<p>Limit requirement for PPP Data Link Layer to switched connections.</p> <p>Add new message types for Reconciliation Reports (364/374).</p> <p>Change tag'C9'to PSAM update flag.</p> <p>Add Field 4 in Authorization Request Response.</p> <p>Add Field 36 for all MSC transactions.</p> <p>Make Field 30 conditional in Authorization Request and Financial Advices.</p> <p>Make Field 47 possible in Financial and Reversal Advices.</p> <p>Add APACS messages for Reconciliation Reports and Messages.</p> <p>Add Reconciliation information to TLV coded information.</p> <p>Add Contactless as entry mode in Field 22</p> <p>Add Contactless and Reconciliation Message Reasons to Field 25.</p> <p>Add tags for Acquirer information in Field 44.</p> <p>Add tags for handling regional requirements and 4 digit CV-2 in Field 47.</p> <p>Add tag for handling of Reconciliation data in Field 63.</p>

		Book 2	Chapter 13	<p>Add Commands for Contactless transactions and Cancellation to Command overview.</p> <p>Add new Identifiers (functions; Extended AID, Reference STAN TVR/TSI/IAC, Contactless Amount, Acquirer Information and Available Funds) to Get Debit/Credit Properties command.</p> <p>Add Contactless as new Card Data Source.</p> <p>Add information on Prepaid Card data to Validate Data 2 command.</p> <p>Convert from track2 data to track 2 or track 3 data.</p> <p>Add Contactless commands, Initiate Contactless Payment, Contactless Payment and Contactless Validate Data</p> <p>Add ASW1-ASW2s for Contactless commands and for new identifiers for the Get Debit/Credit Properties command. Add additional ASW's for declined transactions.</p>
		Book 2	Chapter 14	<p>Add definition of Card Reference.</p> <p>Add definitions for Contactless Prepaid Card concepts.</p>
3.1	2009-12-01	Book 1	Chapter 10	Section 1-10.4 Remove redundant and contradictory requirements for VAT printing.
3.1	2009-12-01	Book 1	Chapter 15	Section 1-15.3 Correct Swedish display and receipt texts.
3.2	2010-12-01	Book 1	General	<p>Change PBS to Nets Denmark A/S.</p> <p>Use underscore under words to identify small changes.</p>
3.2	2010-06-15	Book 1	Chapter 4	<p>New abbreviations, ATM, PCT added.</p> <p>Reference to MSC track3, EMV Contactless Entry Point Specification, Visa Transaction Acceptance Device Requirements/Guide and Maestro preauthorization has been added. APACS 60 and OTTS added in bibliography.</p>
3.2	2010-06-15	Book 1	Chapter 6	<p>New table 1-6.2 (CVM Transaction Type and PSAM version vers. Term.Type) .</p> <p>Table 1-6.3 (Transaction Request Vs. Technology/Card) is added in order to introduce an overview of Debit/Credit as well as Prepaid transactions.</p>
3.2	2010-06-15	Book 1	Chapter 8	Added information on validating the Business Call prior to Initiate Payment.
3.2	2010-06-15	Book 1	Chapter 9	Added information in introduction, that this chapter is informative. Add info on Post Purchase and Post Refund business calls. Add info on Track 3.

				Clarified the description of Get Amount 3.
3.2	2010-06-15	Book 1	Chapter 10	<p>Handling of Extended Authorization updated in 1-10.2.3. Cancellation clarified in 1-10.2.8</p> <p>Private Label Card Scheme handling is specified in section 1-10.4.</p> <p>Terminal Functions renamed to Terminal services in 1-10-5.</p> <p>Updated handling of Account Type Selection in section 1-10.5.3.</p> <p>Clarified the use of Cashback, section 1-10.5.4.</p> <p>Added information on POST registration, i.e. Transactions performed after the normal transaction in 1-10.5.6.</p> <p>Handling of Dual Kernel Configuration, preferred and forced processing added in 1-10.5.8 to 1-10.5.10.</p> <p>Added Prepaid ICC transactions in section 1-10.8.</p> <p>Added note on split payments and prepaid MSC transactions in section 1-10.9.1.</p> <p>Add information on "Verify token" in section 1-10.11.7. Introduce the use of "Card Reference Key" for token transactions in section 1-10.11. Add information on conditions for token and Post Registration in 1-10.10.2</p> <p>Update note on amount to use in macro AUTHORIZE and update flow for macros AUTHORIZE, FINALIZE and AUTHORIZE FOR TIPS in section 1-10.12. Update Figure 1-10.8 1-10.10 and 1-10.13.</p> <p>Clarified content of fields used in DCC transactions in table 1-10.15. Clarified the use of services/extra on DCC transactions in section 1-10.14.</p>
3.2	2010-06-15	Book 1	Chapter 11	Prepaid ICC included where appropriate. Danish terms for Business calls moved to section 1-15.2. Add texts for Post Purchase and Post Refund in table 1-11.2
3.2	2010-06-15	Book 1	Chapter 12	<p>Clarified conditions for printing receipt. Handling of "Card Name" clarified. Text for Post Registration removed in section 1-12.2.6. Handling of track3 added and update on Reference STAN added and printing of ATC clarified in section 1-12.2.9.</p> <p>Printing of TVR and TSI added in section 1-12.2.11.</p> <p>Special receipt requirements for Prepaid ICCs are added in section <deprecated> and other places.</p>

				Handling of Amount, Surcharge and Extra for DCC clarified in section 1-12.3.3.
				Examples of receipts for prepaid ICC cards added in section 1-12.4.
3.2	2010-06-15	Book 1	Chapter 14	Added clarification on the handling of Private Label Card Schemes in 1-14.3.2. New functionality taking the requirements linked to Prepaid ICC into account is added to the section 1-14.3.3 (Building the AID Selection Table).
3.2	2010-06-15	Book 1	Chapter 15	Moved national Danish texts here from section 1-11.2. Add texts for Post Registration in Danish. Generally adjust DCC service provider to "Teller A/S".
				Clarify Swedish terminal services in section 1-15.3.1. Correct spelling errors in display and receipt texts.
				Add Norwegian requirements for regional cards. Add info for AFD's. Add information on specific Norwegian receipt layout. Add requirements for Norwegian reconciliation. Correct spelling errors in display/receipt texts. All in section 1-15.4.
				Add and Update German Display and Receipt texts in section 1-15.6.
3.3.0	2011-06-06	Book 1	Chapter 3 a.s.o.	Rename "Local Card" to "Private Label Card Scheme".
3.3.0	2011-06-06	Book 1	Chapter 4.	CDP has been added to Abbreviations. Add reference to IFSF. The sections References and bibliography have been brought up to date.
3.3.0	2011-07-18	Book 1	Chapter 10	Add information on Additional Card BIN Information and Additional Transaction Information. Update handling of DCC due to PAN truncation.
3.3.0	2011-07-18	Book 1	Chapter 10	The functionality Additional Transaction Information (Extended Issuer Envelope) is added.
3.3.0	2011-07-18	Book 1	Chapter 12, 15	Change (Swedish) Post registration to the generic new token based version.
3.3.0	2011-07-18	Book1	Chapter 15	Remove mandatory requirement for handling of track 3 MSC (Bax) in section 1-15.4. Make availability of reconciliation generation mandatory in attended terminals in Norway.
3.3.0	2011-08-18	Book 1	Chapter 10 a.s.o.	Use concept of "Secure Device" instead of "Tamper Evident Device"
3.3.0	2011-08-18	Book 1	Chapter 15 .	Clarify the requirement for printing of VAT on Swedish receipts.
3.3.0	2011-10-15	Book 1	Chapter 7	Remove PSAM PA-DSS Implementation Guide from the chapter.
3.3.0	2011-10-15	Book 1	Chapter 8	Emphasize that transaction flow is controlled by the PSAM only.

3.3.0	2011-10-15	Book 1	Chapter 9	Update section 9.13 on Data Transmission. Note that DCC and Cashback may not be combined.
3.3.1	2012-03-10	Book1	Chapter 7	Add section 7.1.2 with requirements on centralized security logging.
3.3.1	2012-03-10	Book1	Chapter 10	Update section 10.5.2 with information on additional data for the Extended Issuer Envelope. Add note in section 10.5.11 on limits in the use of forced conditions for some new cards.
3.3.1	2012-03-22	Book1	Chapter 10	Remove section on old prepaid ICC transactions. Allow loading of non-empty MSC cards.
3.3.2	2012-12-01	Book1	Chapter 4	Add new abbreviations. Update references to most recent versions. Add references to contactless cards and transactions.
3.3.2	2012-12-01	Book1	Chapter 5	Add acceptance of contactless transactions.
3.3.2	2012-12-01	Book1	Chapter 6	Add handling of contactless transactions.
3.3.2	2012-12-01	Book1	Chapter 9	Add acceptance of contactless transactions.
3.3.2	2012-12-01	Book1	Chapter 10	Section 10.5.3, allow Account Type Selection based on BIN for ICC. Section 10.5.8 Introduce Acquirer information for all regions. Section 10.6.2. Correct size of PCT body. Section 10.8 Add information for contactless transactions.
3.3.2	2012-12-01	Book1	Chapter 12	Section 12.2.6, remove old post registration text. Section 12.2.8 add texts for contactless and Acquirer merchant information. Clarify source of Status and Auth.code. Section 12.2.11 add handling of AOSA from contactless card. Section 12.4 change reference for prepaid MSC receipts.
3.3.2	2012-12-01	Book1	Chapter 15	Section 15.3 specify exception handling for PCT. Correct error on receipt element AM6. Section 15.4 allow for extra application on BAX. Limit reconciliation. Correct text spelling error. Section 15.8 add Icelandic texts.
3.3.3	2013-01-15	Book1	Chapter 10	Section 10.10 Add handling of Loyalty Information.
3.3.3	2013-01-20	Book1	Multiple	Make reference to EMV specification version independent.
3.3.3	2013-05-22	Book1	Chapter 15	Section 15.3 Remove deprecated data tags. 15.4 Add handling of Bank Asept Exception Rule. Remove requirements for handling of MSC track 3. Clarify requirements for handling of card balance (fuel dispensers). Section 15.5 add Finnish requirements.
3.3.4	2013-08-20	Book 1	Chapter 10	Add section 1-10.5.12 on Electronic Receipts. In 1-10.14.4, add requirement on rejecting DCC in non-DCC terminals.
3.3.4	2013-08-27	Book 1	Chapter 7	Section 7.1.2 Add information on the possible use of security information.

3.3.4	2013-10-03	Book 1	Chapter 4	Add terms related to key encryption.
3.3.4	2013-10-03	Book 1	Chapter 10	1-10.5 electronic Receipt handling. 1-10.14 clarify DCC requirements.
3.3.4	2013-10-03	Book 1	Chapter 12	1-12.2 Add information on "quick" / "easy" payments.
33.4	2013-10-30	Book1	Chapter 15	1-15.5 note on work-around for Online PIN.

This page is intentionally left blank

1-3 Introduction

1-3.1 Overview

1-3.1.1 Audience

This document is intended for terminal suppliers implementing payment terminals using the terminal architecture for PSAM applications, TAPA.

1-3.1.2 Prerequisites

It is assumed that technical readers are familiar with the EMVCo, card scheme specifications, and TAPA and that all readers have a basic understanding of the chip card technology.

1-3.1.3 Scope

The scope of the specification is the functions for which Nets Denmark A/S as a Terminal Operator is responsible, i.e. national and international regulations including the overall security in the terminals.

Terminals are delivered in a relationship between the terminal supplier and the merchant. If the merchant desires enhanced possibilities in the terminal, e.g. "Private Label Cards", the merchant must enter an agreement about this with the terminal supplier. The terminal architecture is defined to be open for other terminal applications and this specification does not prevent the implementation of such applications in the terminal.

The scope of this specification is to provide all functional requirements for a terminal used for card transactions. Design requirements are also stated.

Specific areas of functionality may be limited to, or only utilized by, certain kinds of services, e.g. cashback and return/refund. Some features and restrictions herein are mandated by the Danish legislation.

The terminal architecture is based on the "Terminal Architecture for PSAM Applications (TAPA)" documents see ref. 26 to ref. 28.

1-3.2 Target Group

This specification is for manufacturers intending to develop an OTRS Terminal for accepting debit/credit cards, and/or prepaid cards, and/or other cards.

The terminal may be a stand-alone POS terminal, an integrated EFT-POS environment or a vending machine but server-based solutions are comprised by this specification as well.

1-3.3 Objectives

The purpose of this specification is to enable manufacturers to develop products in such a way that any debit or credit and/or prepaid card based on chip technology and magnetic stripe chip technology can be used for payment for the goods or service offered by the merchant operating the terminal.

The aim of this specification is to enable manufacturers to develop products in such a way that all types of cards can be used.

The main objectives are to read a payment card, check or authorize its validity, perform the cardholder verification and generate an Authorization Request and/or a Financial Advice to be forwarded to the acquirer. The cardholder may in some situations sign a receipt, i.e. use signature as Cardholder Verification Method (CVM) instead of PIN or at special installations like toll gates even perform a transaction without any verification, No CVM.

1-3.4 Level of Detail

This specification is based on a number of documents, e.g. industry specifications like EMV, TAPA, specifications from the international card schemes and PCI (Payment Card Industry, as well as number of international standards from ISO and CEN. These documents shall be read before reading this specification as in order not to have redundant information, this specification does not, as a general rule, copy information in referenced documents.

This specification is described at a level of detail sufficient to develop the entire functionality of the terminal or parts hereof.

The terminal can be developed either as a complete dedicated terminal device or as an integral set of functions in e.g. a customer operated terminal, an electronic POS cash register or a POS terminal.

It has been the aim to describe and specify the POS terminal in "building blocks" making both development and certification easier.

Interfaces are specified in detail. In this way, it is ensured that products from different vendors can interact without interaction between the vendors during the development phase.

Functions are, on the other hand, only specified on a higher level of detail in order not to impose specific implementations.

This specification is aimed for “design for testability”. For this reason, each requirement is individually numbered in order to ease the test and certification of a specific function and its “building blocks”.

Nets Denmark A/S acknowledges that updates of this specification will be made due to input from developers and others. Such feed-back is preferably given in a structured manner.

1-3.5 Document Structure

This specification is organized into two books.

Book 1 encompasses all the general information and is also oriented towards providing overall requirements and information leveled at e.g. manufacturers of cash registers etc. A general revision log for the TRG OTRS and an introduction to this specification is given. Also, a definition of the terms used and a system overview is described.

Book 2 is oriented towards providing specific information, e.g. PSAM commands and responses, leveled at the terminal manufacturers.

The books are supplied as a single electronic document to make it possible to use links between the two books.

This page is intentionally left blank

1-4 Definitions

1-4.1 Introduction

For the purposes of this requirement specification, the abbreviations and specific terms below apply.

The notation used throughout this specification is explained and lists of referenced standards and specifications are given at the end of this chapter.

1-4.2 Terminology

In this specification, some terms are written with a starting capital letter, e.g. Business Call. This is in order to indicate that the term has a particular meaning in connection with this specification although it might otherwise appear quite familiar. Terms used in their traditional meaning within the payment industry are not defined and do not begin with capital letters.

Data elements and commands are also written starting with capital letters. Commands and related responses are defined in chapter 2-14 page 2-14-1, Command and Responses and data elements are defined in chapter 2-15 page 2-15-1, Data Elements.

The following two sections give the definitions and a few supplementary comments on abbreviations and specific terms used throughout this specification.

1-4.2.1 Abbreviations

AID	: Application IDentifier
AAC	: Application Authentication Cryptogram, EMV
AAR	: Application Authorization Referral, EMV
APE	: Accelerated PIN Entry
ARQC	: Authorization Request Cryptogram, EMV
ASN.1	: Abstract Syntax Notation, One
ASI	: Application Selection Indicator
ASW	: Application Status Word
ATM	: Automated teller machine
ATR	: Answer-to-Reset
BDK	: Base Derivation Key
BSK	: Basic Session Key
CA	: Certificate Authority
CAD	: Card Accepting Device
CAM	: Card Authentication Method, EMV
CAT	: Cardholder Activated Terminal (=UPT)
CDA	: Combined DDA/Application Cryptogram Generation, EMV
CDP	: Card Data Protection

CEP	: Common Electronic Purse
CLA	: CLAss byte
CRC	: Cyclic Redundancy Check
CV-2	: Card Verification, method 2
CVM	: Cardholder Verification Method, EMV
CVR	: Cardholder Verification Rule, EMV
DAPE	: Dankort Accelerated PIN Entry
DDA	: Dynamic Data Authentication, EMV
(D)EBS	: (Draft) European Banking Standard, ECBS
DOL	: Data Object List
DS	: Data Store
ECBS	: European Committee for Banking Standards
ECR	: Electronic Cash Register
EFT-POS	: Electronic Funds Transfer at Point of Service
EMV	: Europay, MasterCard and Visa
IC	: Integrated Circuit
ICC	: Integrated Circuit Card (chip card)
ICCR	: Integrated Circuit Card Reader
ICS	: Implementation Conformance Statement
IFD	: Interface Device
IFSF	: International Forecourt Standards Forum
INS	: INStruction code
ISO/IEC	: International Organization for Standardization/ International Electrotechnical Commission
KEK	: Key exchange key / Key Encryption Key
KCV	: Key Check Value
LRC	: Longitudinal Redundancy Check
MAC	: Message Authentication Code
MAD	: Multi-Application Driver (TAPA)
MCC	: Merchant Category Code
MK	: Master Key
MSC	: Magnetic Stripe Card
MSCR	: Magnetic Stripe Card Reader
MSD	: Magnetic Stripe Data
PAN	: Primary Account Number
PBS	: PBS A/S, predecessor to Nets Denmark A/S.
PCI	: Payment Card Industry (PCI SSC)
PCT	: Processing Condition Table
PED	: PIN Entry Device (PIN pad)
PK	: Public Key
PKI	: Public Key Infrastructure
PIN	: Personal Identification Number
POS	: Point of Service
PPK	: PIN Protection Key
PPS	: Protocol and Parameters Selection
PPSE	: Proximity Payment Systems Environment
PSAM	: Purchase Secure Application Module
qVSDC	: Quick VSDC - Visa defined contactless payments mechanism for quick transactions in EMV chip markets
RFU	: Reserved for Future Use
RID	: Registered Application Provider Identifier
PP	: PIN Pad
SAM	: Secure Application Module
SDA	: Static Data Authentication
SDK	: Session Derivation Key
SK	: Secret Key (DES) or Private Key (RSA)
T.B.D.	: To Be Defined
TC	: Transaction Certificate, EMV

TRG : Technical Reference Guide
VPKI : Public Key Index
UPT : Unattended Payment Terminal, PCI

Abbreviations not mentioned here are Data Elements, see chapter 2-15, page 2-15-1.

1-4.2.2 Terms

Authorization,	the validation process which either approves or rejects a payment-transaction on the basis of the rules guiding the use of the payment card. These rules are set by the card issuer.
Business Call,	transaction related information sent from the Merchant Application to the MAD-Handler.
Cardholder Display,	the display for use by the cardholder.
Communication Session,	the communication steps from the terminal initiates a connection, until this session is either closed intentionally or interrupted unintentionally.
Dankort,	the national debit card issued by members of Nets Denmark A/S. Used for purchasing goods and services and for obtaining cash, for which the cardholder's bank account is debited. Visa/Dankort is an affinity card which acts as a normal Dankort when used in Denmark and as a Visa debit card when used abroad.
Early Amount Entry	transactions where the amount is present at the transaction start, i.e. the amount is part of the <i>Initiate Payment</i> command.
Kernel ID	Indicates the card's preference for the kernel on which the contactless application can be processed.
Late Amount Entry	transactions where the amount is <i>not</i> present at the transaction start, i.e. the the PSAM will issue the <i>Get Amount 3</i> command to obtain the amount.
Multi-entry,	functionality in the PSAM which allows several transactions (threads) to be processed "simultaneously".
OTRS Terminal	a card payment terminal. The terminal is developed according to this specification.
Nets PSAM,	the PSAM containing the Nets Denmark A/S defined functionality and encipherment functions including keys, certificates and card selection parameters as well as other data belonging to the Terminal Operator and/or acquirer.
Point of Service,	the merchant location from where the card transaction originates.
Private Label Card	<u>A non-PCI</u> payment card carrying the name of a retailer but actually issued and managed by a third party processor.
Single Unit Terminal,	an attended terminal designed to be operated by both the merchant and the cardholder using the same display and keyboard.

Terminal Operator,	the entity responsible for the surveillance of and the communication with the terminal. The Terminal Operator may also be responsible for maintenance of the Terminal.
Terminal Supplier, Test House,	a supplier of card payment terminals. the entity performing certification of the terminal.
Token,	a string of bytes created by a PSAM as a result of an Authorization transaction. A Token is used as input to a Capture transaction, possibly performed by a different PSAM.
UPT,	Unattended Payment Terminal (UPT) The UPT is a cardholder-operated payment terminal that reads, captures and transmits card information in conjunction with an unattended self-service device, including, but not limited to, the following: <ul style="list-style-type: none"> • Automated Fuel Dispenser • Ticketing Machine • Vending Machine
Transaction,	a complete sequence of events included from an administrative routine or card related Business Call is initiated until the result is known. A Transaction is initiated by either merchant or cardholder. A Transaction may include one or more Communication Sessions.
Visa/Dankort,	a co-badged card which in general act as a Dankort when used in Denmark and as a Visa card when used abroad.
Voice Authorization,	is the procedure used by the merchant to obtain approval for an offline transaction (phone call to the Acquirer's help desk) .

1-4.2.3 Notation

Binary Notation

Whenever a value is expressed in binary form it will be preceded by the characters B and ', e.g. the decimal value 9 is expressed as B'1001.

Bit Numbering

The least significant bit is numbered 0. The number of the bit is increased by one through the bits. The least significant bit is placed rightmost. The most significant bit is placed leftmost. As an example, a binary value has the following bit numbering:

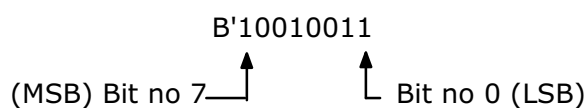


Figure 1-4.1 - Bit Numbering

Hexadecimal Notation

Whenever a value is expressed in hexadecimal form it is surrounded by single quotes.

As an example, the binary value B'01001110 is expressed in hexadecimal as '4E' (78 in decimal notation), and the binary value B'0110101101110101 is expressed as hexadecimal value '6B75' (27509 in decimal notation).

String

Text strings are surrounded by double quotes.

Example: "A string is indicated like this".

Operators

:= Assignment (of a value to a variable).
 $B_1 \parallel B_2$ Concatenation of bytes B_1 (the most significant byte) and B_2 (the least significant byte).

Text Written in Grey

Text written in grey indicates that the concerned section is not applicable, e.g. the function in question is not supported yet.

DES and Triple DES

DES, denoted DES()[], operates on a 64-bit input block and a 64-bit key to produce a 64-bit output block. The number of effective key bits in a DES key is only 56 as every 8th bit of the 64-bit key is a parity bit, thereby ensuring an odd number of "1"s in each key byte.

Triple DES, denoted DES3()[], is implemented using three iterations of the DES block cipher with two independent DES keys K1 and K2.

Specifically, the ciphertext Y of an 8-byte input block X is:

$$Y = \text{DES3}(K1, K2)[X] = \text{DES}(K1)[\text{DES}^{-1}(K2)[\text{DES}(K1)[X]]]$$

Decryption is performed as:

$$X = \text{DES3}^{-1}(K1, K2)[Y] = \text{DES}^{-1}(K1)[\text{DES}(K2)[\text{DES}^{-1}(K1)[Y]]]$$

Attributes for APACS 60 Messages

The following notation is used for data elements for the APACS 60 messages defined in section 2-13:

- a = alphabetic characters, see ref. 12: "ISO/IEC 8859-15"
- b = binary representation of data, measured in bytes
- c = control characters (non-printable and non-displayable): ['00'...'1F', '7F']
- n = numeric digits: [0-9]
- p = pad character (space)
- s = special characters (printable, non-alphanumeric characters, including space): ['20'...'2F', '3A'...'3F', '4B'...'4F', '5B'...'5F', '60', '7B'...'7E']
- z = track 2 (and 3) code set as defined in ref. 4: "ISO/IEC 7811-2:1995", table 7
- MM = month (01...12)

DD	=	day (01...31)
YY	=	year (00...99)
hh	=	hour (00...23)
mm	=	minute (00...59)
ss	=	second (00...59)
LVAR	=	variable length field where the first byte indicates the length of the remaining data in the field as a binary integer
LLVAR	=	variable length field where the first two bytes indicate the length of the remaining data in the field as a binary integer (the leftmost byte is the most significant)
MAX	=	maximum integer for LLVAR fields (65536)

The attributes a, b, c, n, p and s can be combined, e.g. ans means the combination of alphabetic characters, numeric digits and special characters.

NOTE: All fixed length n data elements are assumed to be right justified with leading zeros.

NOTE: All other fixed length data elements are left justified with trailing spaces.

NOTE: In all b data elements, blocks of 8 bits are assumed to be left justified with trailing zeros.

NOTE: All data elements are counted from left to right, i.e. the leftmost position is number 1.

1-4.3 Requirement Numbering

All requirements in this specification are uniquely *numbered* and are *classified* as A-, B- or C-requirements. The first four digits of the number relates to the section where the requirement is stated, whereas the last part is a sequence number.

A-requirements shall always be fulfilled. The word "shall" is used in connection with A-requirements.

B-requirements can only be deviated from, when a proper, written explanation is given to (and accepted by) Nets Denmark A/S. The word "shall" is used in connection with B-requirements.

C-requirements are optional. If they are implemented, the implementation shall, however, follow the guidelines set up in the requirement(s) concerned. The words "may" and "should" are used in connection with C-requirements.

Obtaining waiver(s)

It is only possible to obtain a waiver for B-requirements.

In order to request a waiver please contact Certification of Payment Solutions. Go to the PBS web page, "www.pbs.dk". Select "Products, "Certification". On the Certification web page select "Self-service" and "Waivers"

The information is available in Danish and English.

1-4.4 References

The following documents are referenced in the following chapters of this specification:

1. ISO 4217:2008
Codes for the representation of currencies and funds.
2. ISO 4909:2006
Bank cards - Magnetic stripe data content for track 3
3. ISO/IEC 7810:2003
Identification Cards - Physical characteristics.
4. ISO/IEC 7811-2:2001
Identification cards - Recording technique - Part 2: Magnetic stripe.
5. ISO/IEC 7813:2006
Identification cards - Financial transaction cards.
6. ISO/IEC 7816-1:2011
Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics.
7. ISO/IEC 7816-2:2007
Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts.
8. ISO/IEC 7816-3:2006
Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols.
9. ISO/IEC 7816-5:2004
Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and Registration
10. ISO 8583:1987
Financial transaction card originated messages - Interchange message specifications.
11. ISO 8583:1993
Financial transaction card originated messages - Interchange message specifications.
12. ISO/IEC 8859-15:1999
Information technology - 8-bit single-byte coded graphic character sets - Part 15: Latin alphabet No. 9
13. ISO 9564-1:2011
Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques.
14. ISO 9564-2:2005
Banking - Personal Identification Number management and security - Part 2: Approved algorithm(s) for PIN encipherment.
15. ISO/IEC 9797-1:2011
Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher.
16. EN 726-4:1994
Identification card systems - Telecommunications inte-

- grated circuit(s) cards and terminals - Part 4: Application independent card related terminal requirements.*
17. EN 1332-3:2008
Identification card systems - Man-machine interface - Part 3:Key Pads
 18. ENV 1375:2002
Identification card systems - Intersector integrated circuit(s) card additional formats - ID-000 card size and physical characteristics.
 19. FIPS Publ. 180-1, 1995-04-17
Secure Hash Standard. Also known as SHA-1
 20. EMVCo: EMV Version 4.3 November 2011,
Integrated Circuit Card Specification for Payment Systems:
 - *Book 1: Application Independent ICC to Terminal Interface Requirements;*
 - *Book 2: Security and Key Management;*
 - *Book 3: Application Specification;*
 - *Book 4: Cardholder, Attendant, and Acquirer Interface Requirements*The specification and attached Bulletins can be found at the following address: www.emvco.com.
 21. EMVCo, Contactless Specification for Payment Systems, Version 1.0 May 2008
Entry Point Specification
The specification and attached Bulletins can be found at the following address: www.emvco.com.
 22. EMVCo Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1, March 2011.
 23. EMVCo: *EMVCo Type Approval Contact Terminal Level 2 Administrative Process version 2.2, November 2012.*
 24. EMVCo: *EMVCo Type Approval Contactless Product Administrative Process version 2.2, November 2012.*
 25. APACS Standard 60: 2000-01-01, Version 3
UK Specification for message interchange between Card Acceptor & Acquirer.
 26. Terminal Architecture for PSAM Applications (TAPA), version 2.0, April 2000
Overview
 27. Terminal Architecture for PSAM Applications (TAPA), version 2.1, February 2001
Application Architecture Specification
 28. Terminal Architecture for PSAM Applications (TAPA), version 2.1, February 2001
Application Architecture Specification
Errata version 1.1 2004-03-12
 29. Visa Transaction Acceptance Device Requirements, Version 2.0, March 2011
published by:
Visa International
 30. Visa Transaction Acceptance Device Guide, September 2008, section 5.14.2 *Status check and Account Number Verification*

- published by:
Visa International
31. M/Chip Functional Architecture - For Debit and Credit
June 2011
published by:
MasterCard International Incorporated.
 32. JCB Terminal Requirements
Version 1.0, April 2008
published by:
JCB Co., Ltd
 33. AEIPS Terminal Specification,
(AEIPS 4.1), February 2005
published by:
American Express
 34. Dankort-regler, published by:
Nets Denmark A/S
 35. Payment Card Industry (PCI)
Data Security Standard - Requirements and Security
Assessment Procedures
Version 2.0, October 2010
Published by:
PCI Security Standards Council
 36. Payment Card Industry (PCI):
PIN Transaction Security (PTS)
Device Testing and Approval Program Guide
Version 1.0, September 2010
Published by:
PCI Security Standards Council
 37. Payment Card Industry (PCI)
Payment Application Data Security Standard -
Data Security Standard - Requirements and Security
Assessment Procedures
Version 2.0, October 2010
Published by:
PCI Security Standards Council
 38. MasterCard, Europe Region Operations Bulletin No. 1, 2
January 2008, *Maestro Best-in-Class Programme - Re-
vised Standard for Pre-authorization Solutions for Mae-
stro Petrol Transactions.*
 39. IFSF Standards Part 3-20, IFSF Host to Host Interface.
Version 1.3, May 2006
Published by:
International Forecourt Standards Forum
 40. Nets Design Report:
Card Data Protection
Version 1.09, 2011-10-24
Published by:
Nets Denmark A/S
 41. Visa Contactless Payment Specification (VCPS),
Version 2.1, May 2009.
 42. Visa Contactless Payment Specification (VCPS) 2.1 Up-
dates List,
Version 1, December 2009.
 43. Visa Europe Contactless - Terminal Requirements and
Implementation Guidelines,
Version 1.2, March 2010.

44. MasterCard International, *PayPass* – M/Chip, Technical Specification, Version 2.1.
45. MasterCard Worldwide, *PayPass* – M/Chip Reader Card Application Interface Specification, Version 3.0.1, April 2012.
46. MasterCard Worldwide, *PayPass* – M/Chip Requirements, 5 December 2011.

1-4.5 Bibliography

The following references contain information related to the areas covered by this specification:

47. ISO 639-1:2002
Codes for the representation of names of languages - Part 1: Alpha-2 code.
48. ISO/IEC 7816-4:2005
Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange.
49. ISO 11568-1:2005
Banking - Key management (retail) - Part 1: Principles.
50. ISO 11568-2:2005
Banking - Key management (retail) - Part 2: Symmetric Ciphers, their key management and life cycle.
51. ISO 11568-4:2007
Banking - Key management (retail) - Part 4: Asymmetric cryptosystems - Key management and and life cycle.
52. ISO 13491-1:2007
Banking - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods.
53. ISO 13491-2:2005
Banking - Secure cryptographic devices (retail) - Part 2: Security compliance checklists for devices used in financial transactions.
54. APACS Standard 60:2000
UK specification for Message Interchange between Card Acceptor and Acquirer.
published by:
Association for Payment Clearing Services Ltd.
55. Technical Reference Guide - Open Terminal Integration Test Specification, OTITS
Version 1.0, 2007-03-31
published by:
PBS A/S
56. Technical Reference Guide - Open Terminal Test Specification, OTTS
Version 3.2.0.x, 2012-01-30
to be published by:
Nets Denmark A/S

1-4.6 Related Websites

Related and most recent information may be found at the following websites:

- www.nets.eu
- www.pbs.dk
- www.dankort.dk
- www.mastercard.com
- www.visa.com
- www.emvco.com
- www.ecbs.org
- www.ecbs.com
- www.jcbinternational.com
- www.pcisecuritystandards.org
- www.americanexpress.com
- en.chinaunionpay.com

This page is intentionally left blank

1-5 System Overview

1-5.1 Introduction

This chapter provides the basic overview and prerequisites for reading and understanding this specification. It includes the business requirements ending up as technical requirements in the subsequent chapters.

Rationale for this Terminal Specification

Nets Denmark operates, as a Terminal Operator, an open terminal environment taking the chip card technology into account.

This open environment is a consequence of Nets Denmark A/S' operating terminals handling cards under the brands of American Express, JCB, MasterCard, Visa, and China Union Pay (CUP) as well as prepaid and Private Label Card schemes. This specification obliges with the rules set by these card schemes.

This Technical Reference Guide (TRG) Open Terminal Requirement Specification (OTRS) is developed and maintained by Nets Denmark A/S.

This specification contains the requirements to fulfil when building a terminal with a given profile, e.g. a stand-alone POS terminal for debit/credit cards, or a UPT vending machine for debit/credit cards to be operated in the Nets Denmark A/S environment. This specification does not copy requirements found in e.g. card scheme specifications and standards, though.

As the chip card is the basis for debit and credit cards, the OTRS Terminal must be able to handle such cards according to the EMV specifications issued by EMVCo.

1-5.2 Standards

The terminal infrastructure consisting of terminals and communications network as well as acquirer and issuer host systems has been created in order to accept chip cards.

The basis for all these components are international standards as well as application-specific specifications.

International Standards

Wherever feasible, this specification is based on international standards for chip cards and for magnetic stripe cards as well as for cryptography and data communication.

EMV (Debit/Credit Applications)

The international card schemes have pushed the move to use chip cards throughout the industry.

The debit/credit cards are implemented as applications on the chip according to the EMV specifications issued by EMV-Co.

As a consequence, all terminals and related infrastructure must be enabled to accept such chip cards.

Terminal Architecture for PSAM Applications (TAPA)

This specification is an application specification based on the TAPA specification (“Terminal Architecture for PSAM Applications”).

NOTE: A PSAM (Purchase Secure Application Module) is a security module handling at least the cryptographic functions in the terminal. The PSAM is further described in section 2-3.1 page 2-4-1.

TAPA defines the architecture of a terminal as a number of handlers which can interact. It also defines commands and responses to be supported by each handler as well as standardized response codes.

TAPA was developed jointly by MasterCard, Visa and PBS.

Relationships between Involved Documents

The main standards and specifications relevant for OTRS are shown in figure 1-5.1 where the documents named TAPA are the common documents for the open terminal architecture.

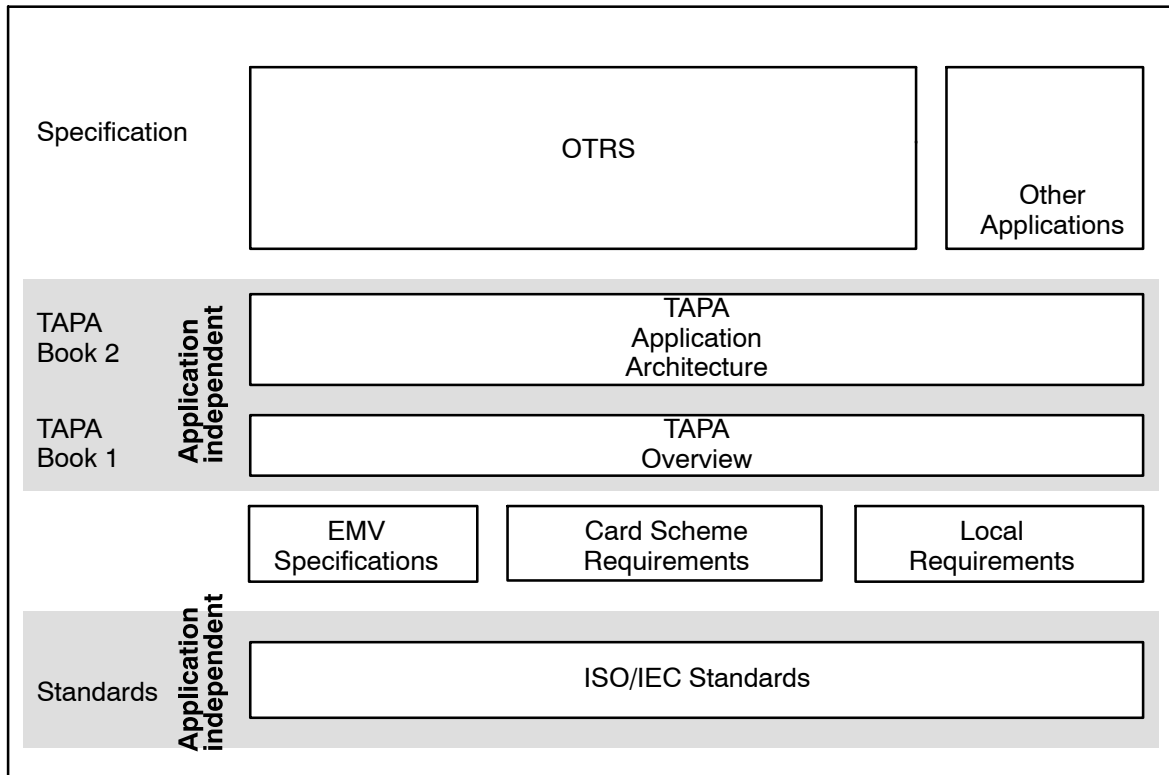


Figure 1-5.1 - Document relationships

The foundation is the international standards referenced and extended by the application specific de facto standards, such as EMV.

Local market requirements are not defined in the international standards and general specifications issued by the card schemes. Such local market requirements are included in this specification

As this specification, TRG-OTRS, is based on all the documents and requirements mentioned above, the implementer of an OTRS terminal needs the knowledge of all referenced documents in order to be able to successfully develop an OTRS terminal.

1-5.3 Business Requirements

The basic type of an OTRS terminal built according to this specification contains as a minimum the debit/credit application. The TAPA terminal architecture supports multiple applications in a terminal, and the terminal manufacturer may implement other applications e.g. loyalty applications according to agreement with the merchant.

The debit/credit application is specified to operate within current card scheme operational and functional requirements. As such, changes to requirements may be introduced accordingly. Also ongoing development of the Single Euro(pean) Payment Area, SEPA, has created and will create new requirements and specifications as e.g. the EPC Smart Card Framework and the SEPA Cards Standardisation Volume.

This version of the TRG - OTRS introduces definitions and terminology as defined in the SEPA Cards Standardisation Volume to some extent.

The terminal specified in this specification may be implemented in various ways, all fulfilling some or all of the business requirements particular to a given merchant.

The overall requirements for the debit/credit application are listed below in these groups:

- Payment Services
- Acceptance Technologies
- Acceptance Environments
- Cardholder Verification Methods
- Card Authentication Methods
- Functions

NOTE: Applications not covered by this specification, such as loyalty applications and payment applications for other card schemes, can co-exist with the applications defined here.

1-5.3.1 Payment Services

As the basis for the OTRS terminal is the debit/credit application, the terminal shall offer one or more of the specified payment services depending on the acceptance environment and merchant/market requirements:

- Payment
 - o Payment
 - o Payment with increased amount
 - o Payment with cashback
 - o Payment with dynamic currency conversion
 - o Payment with additional card data
 - o Payment with cumulative amount
 - o Payment with deferred clearing
 - o Payment with loyalty information
- Refund
 - o Full amount
 - o Partial amount
- Cancellation
- Pre-authorization
 - o Original Authorization
 - o Supplementary Authorizations
 - o Reversal of Authorizations
- Deferred payment
- No-Show
- Instalment payment
- Recurring payment
- Quasi-cash payment

A number of additional services may be offered e.g. in banks or for pre-paid (gift) cards:

- Cash
 - o Cash advance
 - o Cash deposit
- Card inquiry
 - o Card validity check
 - o Balance inquiry
- Card electronic transfer
 - o Card funds transfer
 - o Original credit
 - o Pre-paid card loading
 - o Pre-paid card unloading
 - o (E-purse loading/unloading)

Other payment services are currently out of scope for this specification of the debit/credit application.

1-5.3.2 Acceptance Technologies

The OTRS terminal is specified to use one or more of the following acceptance technologies:

- ICC (EMV) with contacts
- ICC (EMV) contactless (*PayPass* or *payWave*)
- Magnetic stripe
- Contactless MSD (*PayPass*)
- Manual entry
- (Proximity with mobile)

Other acceptance technologies are currently out of scope of this specification.

1-5.3.3 Acceptance Environments

The OTRS terminal is specified to be operated in one of these acceptance environments:

- Attended
- Unattended

- Semi-attended

Other environments e.g. proximity payment and remote payment (MOTO) are currently out of scope of this specification.

For descriptions of terminal types and environments, see chapter 1-6 page 1-6-1.

1-5.3.4 Cardholder Verification Methods

The following cardholder verification methods, CVM, are specified to be used in the OTRS terminal depending on the acceptance environment:

- Offline clear text PIN
- Offline enciphered PIN
- Online PIN
- Signature
- No CVM

Other cardholder verification methods e.g. biometrics are currently out of scope of this specification.

1-5.3.5 Card Authentication Methods

The following card authentication methods, CAM, are specified to be used in the OTRS terminal depending on the acceptance environment:

- EMV SDA
- EMV DDA
- EMV CDA
- Online authorization
- (Remote card/token authentication)
- (Card security code)

Other card authentication methods are currently out of scope of this specification.

1-5.3.6 Functions

A payment service is based upon the functions available in the OTRS terminal. The following functions are specified:

- Account type selection
- Application Selection
- Authorization (total and partial)
- Card authentication
- Card data retrieval
- Cardholder authentication
- Completion
- Configuration
- Data capture
- Financial presentment
- Language selection
- Reconciliation
- Referral
- Reversal (partial and total)
- Technology selection

These functions and their functional specifications are detailed later in this specification.

1-5.3.7 Terminal Types

For the debit/credit application, EMVCo has defined a range of terminal types. These are described in section 1-6 page 1-6-1.

1-5.4 Certification of Terminals

An OTRS terminal developed according to this specification shall be fully tested and the payment application and PIN Entry Device, PED shall be security evaluated according to the Payment Card Industry standards before the terminal is installed for operation.

See the Nets Denmark A/S web-page regarding the certification of terminals and payment solutions:

<http://www.nets.eu>

See the EMV web-page regarding of the EMVCo certification of the terminal:

<http://emvco.com>

See the PCI Security Standards Council for the security standards and evaluation procedures:

<https://www.pcisecuritystandards.org>

1-6 Terminal Types and Environments

The OTRS terminal should be implemented according to the environment it intended to operate in.

Each environment has its own specific needs and requirements to the functions in the terminal.

This section intends to create an overview of the terminal types and their implementation profiles according to environments.

1-6.1 Terminal Types

The acceptance of transactions takes place in different types of terminals and environments accepting both chip cards and magnetic stripe cards.

This specification is used irrespective of the actual implementation of the terminal, e.g. the terminal may be a physical device on the merchant's desk, a vending machine, an integrated part of the software in a hotel system, or a remote device connected to a back office system.

Another main distinction between environments is whether the terminal is unattended or attended, i.e. whether the cardholder operates the terminal by himself/herself or is assisted by the merchant.

The Retail Environment

The retail environment is typically where a stand-alone terminal accepting debit/credit is installed and operated as an attended terminal.

The stand-alone terminal may be installed as a separate terminal at the Point of Service (POS) or as an integrated terminal as an add-on device to an electronic cash register.

Unattended Payment Terminals (UPT)

The unattended payment terminals may have different capabilities and requirements depending on the actual environment and terminal.

Restaurants, Hotels and Car Rental

The handling of card based payments in restaurants, hotels and car rentals are often different from normal retail environments. One example could be restaurants where the possibility of paying a gratuity must be included. Other examples are hotels and car rental companies, where the payment is performed at check-out without the cardholder being present. The payment is based on the card authorization done at check-in/pick-up.

Fuel Dispensers

A payment transaction at an unattended fuel dispenser consists of two phases. First, the card is pre-authorized using an

estimated transaction amount. If this completes successfully, the fuel pump is opened.

When refuelling is done, the exact transaction amount is known, and the actual payment transaction is generated based on card data stored when the authorization was performed. The physical card need not be present during this phase.

Cash Advance Terminals

Specific rules concerning floor limits, fees, cardholder verification, etc. apply to cash advance transactions. By setting parameters in the terminal and the PSAM, these rules can be obeyed in such environments, e.g. terminals installed in bank branches.

1-6.1.1 Terminal Environments, Debit/Credit

Participants

The major participants involved in a debit/credit transaction are:

- The cardholder
- The merchant
- The Terminal Operator
- The acquirer
- The card issuer

The roles of these participants are briefly described below.

Cardholder

The cardholder has made an agreement with a card issuer (typically a bank) to use a debit/credit card to access his/her account. Certain limitations may implicitly be imposed by the card scheme in question or explicitly imposed in the agreement, e.g. amount limits and allowed transaction types and locations.

Merchant

The merchant operates the terminal under agreement with the Terminal Operator(s) as well as one or more acquirers.

Different terminal applications may use different Terminal Operators but in this case, there may be limitations in the use of PINs as described in section 2-3.4 page 2-4-9.

Terminal Operator

The Terminal Operator controls one or more PSAMs/applications in the terminal and switches transactions from the terminal to one or more acquirers. When doing this, transaction data may be reformatted and re-enciphered depending on the formats defined by each acquirer.

The Terminal Operator updates operational data elements in the PSAMs on behalf of the acquirers.

The Terminal Operator may provide statistical data to the merchant on turnover per card type, failure rates etc.

Finally, the Terminal Operator may download updated versions of the terminal software on behalf of the Terminal Supplier.

Acquirer

The acquirer is responsible for obtaining the necessary transaction authorizations from the card issuers and to convey settlement information to and from the card issuers.

The acquirer is furthermore responsible for settlement with the merchant.

Card Issuer

The card issuer provides the card (or card application) to the cardholder. The card issuer also authorizes individual online transactions to limit the risk.

Funds are transferred to the acquirer, either directly or via a card scheme, such as Visa, MasterCard, JCB or China Union-Pay.

Delegation

The roles and responsibilities of the participants described above are the foundation for this specification. However, in a given implementation, specific tasks may be performed by a different entity than the one defined here for that task. This principle is known as delegation and shall be agreed upon by Nets Denmark A/S in each case.

Basic Interconnections

As depicted in figure 1-6.1, the scope for this specification and the environment in which the terminal will operate is limited to defining the requirements to be met when Nets Denmark A/S is the Terminal Operator. Depending on the card type, Nets Denmark A/S may additionally be acquirer and possibly also card issuer or act on behalf of an acquirer and/or card issuer.

The terminal may connect to Terminal Operators other than Nets Denmark A/S for other applications (not involving the Nets Denmark A/S PSAM).

The physical network between the terminal and Nets Denmark A/S as the Terminal Operator is not defined but left to the agreement between two parties; the merchant and the Terminal Operator. Record formats however are defined in detail in this specification.

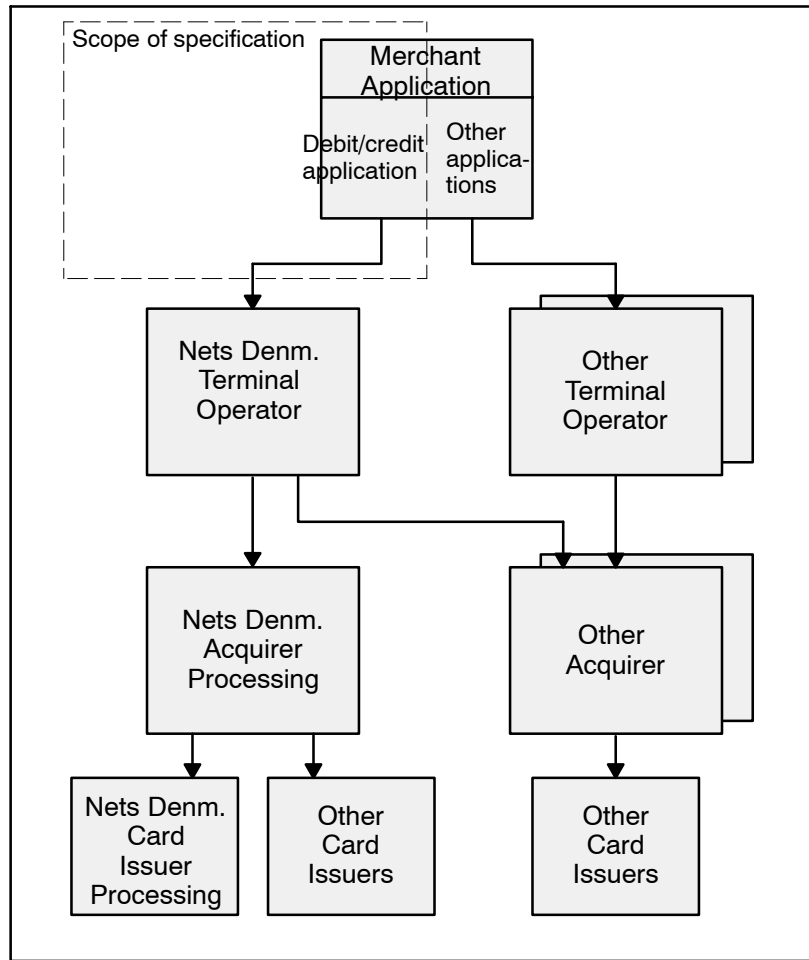


Figure 1-6.1 - Network Model, Debit/Credit

1-6.1.2 Cardholder Verification Methods

The OTRS terminal may support all or some of the EMV defined cardholder verification methods. See ref. 20: "EMV ICC Specification".

1-6.2 Cash/Quasi-Cash Terminals

The following combinations of Terminal Types and Transaction Types are supported:

Table 1-6.1 - Cash/Quasi-Cash Terminals

Terminal Type	Transaction Type	Merchant Category
11 (Cash, Financial Institution)	01 (Cash)	Banks & savings banks (6010)
21 (Quasi-Cash)	11 (Quasi-Cash)	Gambling & Casino (7995) Exchange bureau (6051) Post office (4829)

Cash Terminals have the following limitations:

- Cash transactions are *always* performed online
- PIN and Signature are allowed as CVM
- Refund transactions are *not* allowed
- Cash can *not* be combined with Goods and Services

Quasi-Cash Terminals have the following limitations:

- Quasi-Cash transactions are *always* performed online
- PIN and Signature are allowed as CVM
- Quasi-Cash can *not* be combined with Goods and Services

1-6.3 POS Terminal/UPT Levels vs. Terminal Type

The following two tables (1-6.2 - 1-6.3) can be used to find the outer boundaries for a specific Terminal Type regarding of-line/online transactions, CVM, Transaction Requests and Transaction Type.

Note that terminals may be limited further due to specific restrictions (international as well as national). Therefore, it is highly recommended to contact Nets Denmark A/S before finalizing the terminal functionality design.

NOTE: Signature only terminals are *not* allowed if it is expected that the terminal shall process card brands from MasterCard International and Visa International.

This page is intentionally left blank

Table 1-6.2 - Terminal Types

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Attended – Financial Institution Controlled (Terminal Type 11 – Online only)													
TR00	Purchase	TT01	Cash	V50	V50			V50	■	■	■		
TR00	Purchase	TT09	Cashback										
TR01	Refund	TT20	Returns/Refunds	V53	V53			V53			■ 2)		
TR02	Original Auth.	TT01	Cash	V50	V50			V52	■	■	■ 3)		
TR03	Suppl. Auth.	TT01	Cash										
TR04	Capture	TT01	Cash	V50	V50						■		
TR05	Reversal	TT01	Cash	V50	V50								
TR06	Cancellation	TT01	Cash	V60	V60								
TR07	Extend. Auth.	TT01	Cash	V60	V60			V60	■	■	■		
TR09	Extend Auth. 2	TT01	Cash	V70	V70			V70	■	■	■		
<p>Legend:</p> <p>VXX: Minimum PSAM version</p> <p>Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)</p> <p>Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.</p> <p>TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.</p> <p>TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.</p> <p>Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.</p> <p>1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.</p> <p>2) = Merchant signature.</p> <p>3) = Signature is given when the Capture is performed.</p>													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Attended – Merchant Controlled (Terminal Type 21 – Online only)													
TR00	Purchase	TT11	Quasi-Cash	V50	V50			V50	■	■	■		
TR00	Purchase	TT09	Cashback										
TR01	Refund	TT20	Returns/Refunds										
TR02	Original Auth.	TT11	Quasi-Cash										
TR03	Suppl. Auth.	TT11	Quasi-Cash										
TR04	Capture	TT11	Quasi-Cash										
TR05	Reversal	TT11	Quasi-Cash										
TR06	Cancellation	TT11	Quasi-Cash	V60	V60								
TR07	Extend. Auth.	TT11	Quasi-Cash										
TR09	Extend Auth. 2	TT11	Quasi-Cash										
Legend:													
VXX: Minimum PSAM version													
Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)													
Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.													
TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.													
TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.													
Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.													
1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.													
2) = Merchant signature.													
3) = Signature is given when the Capture is performed.													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Attended – Merchant Controlled (Terminal Type 22 – Offline with online capability)													
TR00	Purchase	TT00	Goods and Services	V50	V50	V53		V50	■	■	■	■	
TR00	Purchase	TT00	Goods and Services				V80		■ ¹⁾		■	■	□ 8.00.03
TR00	Purchase	TT09	Cashback	V70	V70			V70	■	■	■	■	
TR00	Purchase	TT09	Cashback				V80		■ ¹⁾		■	■	□ 8.00.03
TR01	Refund	TT20	Returns/Refunds	V50	V50	V53	V80	V53			■ ²⁾		□ 8.00.03
TR02	Original Auth.	TT00	Goods and Services	V50	V50	V53		V52	■	■	■ ³⁾	■	
TR03	Suppl. Auth.	TT00	Goods and Services	V50	V50	V53							
TR04	Capture	TT00	Goods and Services	V50	V50	V53					■		
TR05	Reversal	TT00	Goods and Services	V50	V50	V53							
TR06	Cancellation	TT00	Goods and Services	V60	V60	V60	V80						□ 8.00.03
TR07	Extend. Auth.	TT00	Goods and Services	V60	V60			V60	■	■	■	■	
TR09	Extend. Auth. 2	TT00	Goods and Services	V70	V70			V70	■	■	■	■	
TR0A	Post Purchase	TT00	Goods and Services	V70	V70	V70						■	Key Entered (Token based)
TR0B	Post Refund	TT20	Returns/Refunds	V70	V70	V70					■ ²⁾		Key Entered (Token based)
Legend:													
VXX: Minimum PSAM version													
Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)													
Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.													
TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.													
TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.													
Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.													
1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.													
2) = Merchant signature.													
3) = Signature is given when the Capture is performed.													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Attended – Merchant Controlled (Terminal Type 22 (without PIN Pad) – Offline with online capability)													
TR00	Purchase	TT00	Goods and Services	V50	V50	V53		V50			■		
TR00	Purchase	TT09	Cashback	V70	V70	V70		V70			■		
TR01	Refund	TT20	Returns/Refunds	V53	V53	V53		V53			■ 2)		
TR02	Original Auth.	TT00	Goods and Services										
TR03	Suppl. Auth.	TT00	Goods and Services										
TR04	Capture	TT00	Goods and Services										
TR05	Reversal	TT00	Goods and Services										
TR06	Cancellation	TT00	Goods and Services	V60	V60	V60							
TR07	Extended Auth.	TT00	Goods and Services										
TR08	Top Up	TT00	Goods and Services										
TR09	Extend. Auth. 2	TT00	Goods and Services										
Legend:													
VXX: Minimum PSAM version													
Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)													
Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.													
TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.													
TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.													
Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.													
1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.													
2) = Merchant signature.													
3) = Signature is given when the Capture is performed.													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Unattended – Merchant Controlled (Terminal Type 24 – Online only)													
TR00	Purchase	TT00	Goods and Services	V50	V50			V50	■				
TR00	Purchase	TT09	Cashback										
TR01	Refund	TT20	Returns/Refunds										
TR02	Original Auth.	TT00	Goods and Services	V50	V50			V52	■				
TR03	Suppl. Auth.	TT00	Goods and Services	V50	V50								
TR04	Capture	TT00	Goods and Services	V50	V50								
TR05	Reversal	TT00	Goods and Services	V50	V50								
TR06	Cancellation	TT00	Goods and Services	V60	V60								
TR07	Extend. Auth.	TT00	Goods and Services	V60	V60			V60	■				
TR08	Top Up	TT00	Goods and Services										
TR09	Extend Auth. 2	TT00	Goods and Services	V70	V70			V70	■				
Legend:													
VXX: Minimum PSAM version													
Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)													
Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.													
TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.													
TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.													
Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.													
1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.													
2) = Merchant signature.													
3) = Signature is given when the Capture is performed.													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Unattended – Merchant Controlled (Terminal Type 25 – Offline with online capability)													
TR00	Purchase	TT00	Goods and Services	V50	V50			V50	■	■			
TR00	Purchase	TT09	Cashback										
TR01	Refund	TT20	Returns/Refunds										
TR02	Original Auth.	TT00	Goods and Services	V50	V50			V52	■	■			
TR03	Suppl. Auth.	TT00	Goods and Services	V50	V50								
TR04	Capture	TT00	Goods and Services	V50	V50								
TR05	Reversal	TT00	Goods and Services	V50	V50								
TR06	Cancellation	TT00	Goods and Services	V60	V60								
TR07	Extend. Auth.	TT00	Goods and Services	V60	V60			V60	■	■			
TR08	Top Up	TT00	Goods and Services										
TR09	Extend. Auth. 2	TT00	Goods and Services	V70	V70			V70	■	■			
Legend:													
VXX: Minimum PSAM version													
Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)													
Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.													
TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.													
TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.													
Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.													
1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.													
2) = Merchant signature.													
3) = Signature is given when the Capture is performed.													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Unattended – Merchant Controlled (Terminal Type 25 (without PIN Pad) – Offline with online capability)													
TR00	Purchase	TT00	Goods and Services	V50	V50			V50				■	
TR00	Purchase	TT09	Cashback										
TR01	Refund	TT20	Returns/Refunds										
TR02	Original Auth.	TT00	Goods and Services	V50	V50							■	
TR03	Suppl. Auth.	TT00	Goods and Services	V50	V50								
TR04	Capture	TT00	Goods and Services	V50	V50								
TR05	Reversal	TT00	Goods and Services	V50	V50								
TR06	Cancellation	TT00	Goods and Services	V60	V60								
TR07	Extend. Auth.	TT00	Goods and Services	V60	V60							■	
TR08	Top Up	TT00	Goods and Services										
TR09	Extend. Auth. 2	TT00	Goods and Services	V70	V70							■	
<p>Legend:</p> <p>VXX: Minimum PSAM version</p> <p>Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)</p> <p>Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.</p> <p>TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.</p> <p>TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.</p> <p>Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.</p> <p>1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.</p> <p>2) = Merchant signature.</p> <p>3) = Signature is given when the Capture is performed.</p>													

Transaction Request		Transaction Type		Original Card Data Source				Late Amount Entry	Cardholder Verification Methods (CVM)				Comments
TRXX		TTXX		EMV	MSC	Key Entered	Contact-less		Online PIN	Offline PIN	Signature	No CVM	
Unattended – Merchant Controlled (Terminal Type 26 – Offline only)													
TR00	Purchase	TT00	Goods and Services	V50	V50			V50				■	
TR00	Purchase	TT09	Cashback										
TR01	Refund	TT20	Returns/Refunds										
TR02	Original Auth.	TT00	Goods and Services										
TR03	Suppl. Auth.	TT00	Goods and Services										
TR04	Capture	TT00	Goods and Services										
TR05	Reversal	TT00	Goods and Services										
TR06	Cancellation	TT00	Goods and Services	V60	V60								
TR08	Top Up	TT00	Goods and Services										
TR07	Extended Auth.	TT00	Goods and Services										
Legend:													
VXX: Minimum PSAM version													
Cashback: Supported for PSAM V70 and higher. The PSAM will modify the Transaction Type to TT09 (Goods and services with cash disbursement)													
Cancellation: Cancellation is applicable only for previously performed successful Purchase transactions.													
TERM22 (without PIN Pad – Signature only): Accepts Dankort/VisaDankort only.													
TERM25 (without PIN Pad – No CVM): Accepts Dankort/VisaDankort only.													
Grey boxes: Option <i>not</i> supported currently. If the grey box contains a version number, the functionality is supported by the PSAM, but not by the terminal/host.													
1) = Consumer Device CVM/On Device Cardholder Verification is also a possibility.													
2) = Merchant signature.													
3) = Signature is given when the Capture is performed.													

Table 1-6.3 - Transaction Request Vs. Technology/Card

Technology/Card ⚡ Transaction Request (TR) ⚡	ICC Contact		ICC Contactless		MSC		Key Entered	
	Debit/Credit	Prepaid	Debit/Credit	Prepaid	Debit/Credit	Prepaid	Debit/Credit	Prepaid
00 – Purchase	☞		☞1)		☞		☞	
01 – Refund	☞		☞1)		☞		☞	
02 – Original Auth.	☞				☞		☞	
03 – Suppl. Auth.	☞				☞		☞	
04 – Capture	☞				☞		☞	
05 – Reversal (Auth.)	☞				☞		☞	
06 – Cancellation	☞2)		☞1)2)		☞2)		☞2)	
07 – Extended Auth.	☞				☞			
09 – Extended Auth. 2	☞				☞			
0A – Post Purchase	☞				☞		☞	
0B – Post Refund	☞				☞		☞	

Legend:
☞ = Supported, ☒ = Supported by the PSAM, but not by the host/terminal.
Grey boxes: Option *not* supported currently.
1) = Does as well cover MSD (*PayPass*).
2) = Can be performed up to 10 minutes after a successful Purchase.

This page is intentionally left blank

1-7 Payment Card Industry - Data Security Standard

1-7.1 PCI - DSS

The PCI Security Standards Council, PCI SSC issues and maintains standards specifying relevant security requirements for systems that store, process or transmit card data and other sensitive data e.g. PINs.

These standards include a general requirements specification ref. 35: "Payment Card Industry (PCI), Data Security Standard", PCI DSS, the related sub standard ref. 37: "Payment Card Industry (PCI), Payment Application Data Security Standard", PA-DSS, and ref. 36: "Payment Card Industry (PCI), PIN Entry Device (PED) Standard", PA-PED.

This section describes how the PCI DSS and PA-DSS requirements may influence on the actual implementation of selected functions described elsewhere in OTRS.

Also, the Nets PA-DSS Implementation Guide for the Nets PSAM can be provided by request from the Nets Denmark A/S Product Compliance department.

The requirements in the PCI documents are not tested during the Nets Denmark A/S certification. PCI assessments are performed by an PCI approved QSA/PA-QSA. Please contact the Nets Denmark A/S Product Compliance department for information on the validation requirements for terminal vendors and resellers/integrators. This assessment is the responsibility of the the terminal vendor (PA-DSS) and the merchant (DSS).

1-7.1.1 Priority of PCI SSC Standards

The general guidelines stated in this section may, due to changes in PCI SSC standards e.g. the PCI DSS and PA-DSS requirements, introduce a contradiction between the requirements stated in this specification and the standards defined by PCI SSC.

The PCI SSC standards are relevant for all transactions processed by an OTRS terminal or forwarded to Nets Denmark A/S for switching or acquirer processing.

NOTE: In case of contradiction between PCI SSC standards and any requirements stated in the OTRS (including requirements in this section), the PCI SSC standards are first priority.

1-7.1.2 Centralized log handling

The PCI PA-DSS requires the access to a centralized log service for the Merchant. This subclause specifies the requirements for log file handling.

- 1-7.1.2.11 A The terminal shall, whenever it receives an ASW of '6x xx' or '11 2x' from the PSAM, retrieve the value. The value shall be converted to ASCII text, framed and forwarded to the centralized Merchant log environment.
- 1-7.1.2.12 C The data should be formatted as; "ASW:nnnn".

1-7.1.3 Receipts and Truncation of the PAN

The requirements for truncation of PAN when printed on cardholder receipts are stated in section 1-12.2.9. The general requirement is that the PAN shall be truncated when printed on receipts handed over to the cardholder.

However, in certain business environments, e.g. if the cardholder accepts the transaction by signature, a receipt for the merchant files may be printed including the full card number.

A receipt copy printed for the merchant files may also be used as back-up. E.g. if an offline PIN has been entered, but no online authorization has been performed, a merchant receipt showing the complete PAN may be necessary for documentation purpose.

- 1-7.1.3.1 C The PAN may be printed in clear text on receipts intended to be stored in the merchant files as individual paper sheets.

NOTE: Such receipts must be stored in accordance with PCI DSS requirements.

- 1-7.1.3.2 A If all digits of the PAN are printed as visible text on merchant receipts, the data printed shall NOT be stored electronically, unless the storage media is protected according to the PCI DSS requirements.

- 1-7.1.3.3 A If all digits of the PAN are printed visible on the merchant receipts, the receipt data shall not leave any copies of the PAN in memory after use.

- 1-7.1.3.4 A If the receipt printer is connected to the electronic cash register, the transfer of the receipt from the terminal to the printer shall not leave any unprotected copies of the PAN in the cash register system or printer.

NOTE: PCI DSS applies to all systems that *store, process, or transmit* card data.

1-7.1.4 Transaction Log

The general requirements for the Transaction Log are stated elsewhere in the OTRS.

The Transaction Log may be generated and stored in either the terminal or a connected cash register system (Merchant Application).

- 1-7.1.4.1 A If the Transaction Log contains data elements covered by the PCI DSS requirements, the implementation shall meet the relevant PCI DSS and PA-DSS requirements.

- 1-7.1.4.2 C It is recommended that the information printed on cardholder receipts comprises the card and transaction information stored in the Transaction Log.
- 1-7.1.4.3 A If the full PAN is printed in clear text on the corresponding cardholder receipt, the information shall be truncated or protected by other means in the Transaction Log as per PCI DSS requirements.

1-7.1.5 Tools for transaction follow-up

If the transaction flow from the terminal to the acquirer is interrupted due to any technical problems, and one or more transactions are not cleared and settled as expected, an investigation may be initiated.

All relevant parties may take an active share in the investigation, but a minimum set of data elements shall be available to complete the investigation.

If the result of the investigation indicate that a 'repeat' of the original and lost transactions shall be initiated, the PAN must be part of the data elements available.

A receipt copy printed for the merchant files may be used as back-up, e.g. if offline PIN has been entered, but no on-line authorization has been performed. In this situation no information from the actual card can be found in the host systems before the financial advice is transferred.

If the PAN is obtained from paper receipts, the description concerning truncation of PAN on receipts applies.

The Merchant Log is described in details in section 1-14.10 in this specification. The Merchant Log is intended to be used as a back-up of transaction advices which have financial impact. Errors may give rise to situations where the original message is not transferred correctly from the Data Store. A tool for finding and transferring such advices may be developed by the terminal vendor.

- 1-7.1.5.1 B If a service tool for finding and transferring advices from the Merchant Log is implemented, this tool shall offer a function by which only selected advices can be transferred.
- 1-7.1.5.2 B If the Merchant Log is implemented, the advices stored in this log shall be deleted from the log, when the back-up is no longer needed.

NOTE: Since the advices stored in the Merchant Log are enciphered by the PSAM, the Merchant Log may be established where applicable in the sales system.

NOTE: PCI DSS requirements apply to all systems that store, process or transmit data, *even if the data is encrypted.*

1-7.1.6 Handling of PAN in Merchant Application

In certain environments the Merchant Application (e.g. in the cash register system) needs to identify the actual card in use before the transaction processing may continue.

Example: The Merchant Application may add surcharge to the amount to pay for goods and services, before the total amount is sent to the terminal. Addition of surcharge requires that the Merchant Application is able to identify the actual card, and based on this information calculate the correct additional amount before transfer to the terminal.

Identification of the actual type of card may also be relevant for the processing and settlement in the merchants account departments.

The Merchant application may identify the actual card based on the PAN or part of the PAN.

Identification based on other data elements than the PAN is outside the scope of the OTRS.

- | | | |
|-----------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-7.1.6.1 | B | If the identification of the actual card is based on a limited part of the PAN (e.g. the first n digits of the PAN), the number of digits visible on a display shall meet the PCI DSS requirements concerning truncation of card data. |
| 1-7.1.6.2 | B | If the identification is based on the complete PAN, the PAN shall NOT be stored electronically, unless the storage media is protected according to the PCI DSS and PA-DSS requirements. |
| 1-7.1.6.3 | B | If the complete PAN is transferred to the Merchant Application, the transfer and processing shall not leave any copies of the PAN in memory after use. In addition, the merchant application must be protected in accordance with PCI DSS and PA-DSS requirements. |
| 1-7.1.6.4 | B | If the PAN is transferred as part of the data element Track2 Data, the above requirements concerning transfer of the complete PAN apply. |

1-7.1.7 Handling of Track2 Data

If the transaction processing is based on reading of the magnetic stripe from the card, only the data element Track2 Data is available.

Track2 Data contains the PAN and a number of other data. Generally, the optional Expiry Date and Service Code comprise the first 7 digits after the PAN and the Separator.

- | | | |
|-----------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-7.1.7.1 | B | If the transaction is based on reading the magnetic stripe, the contents of Track2 Data shall be limited before the data is transferred to e.g. the Merchant Application for identification. |
|-----------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

NOTE: Generally, only the PAN (or the prefix of the PAN) is needed to be able to identify the actual type of card.

- | | | |
|-----------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-7.1.7.2 | B | The complete Track2 Data shall not be used as input to any processing other than input to the PSAM. Refer to PCI DSS and PA-DSS for further information on the handling and protection of Track2 and other sensitive authentication data. |
|-----------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1-7.1.8 Handling of Key Entered card data

If the transaction processing is based on key entering of card data, the following three data elements should comprise the data available: PAN, Expiry Date and CV-2.

Key entering of card data is normally performed on the Merchant Application.

- 1-7.1.8.1 B Key entry of card data, preliminary processing and transfer to the terminal for further processing in the PSAM shall meet the requirements defined in PCI DSS and PA-DSS.

1-7.1.9 Use of derived identification

In certain environments the actual payment card may be used as an identification of the actual customer or the goods that is the subject of the purchase.

The following list of non-exhaustive examples identifies environments where the card may be used as identification:

- In self service petrol stations, the payment process is initiated before fuelling the car, but the receipt is not available until the fuelling is completed. The cardholder may request the receipt to be printed by inserting the card again after filling. To be able to find the receipt in the queue of receipts, a unique identification of the card is needed.
- In self service parking areas, the card is identified and controlled at the time of entry. When the cardholder exits the parking area the card is used as identification for the calculation of the parking time. The payment is then initiated.
- At the time of check-in at a hotel, a pre-authorization of the card is performed and the transaction data is saved for later completion of the payment when the amount is known. The cardholder may be identified at the time of check-out by reading the card again

The PAN including the PAN sequence number is the only unique data element in all cards. A unique identification parameter may be derived from the actual PAN and other data elements.

- 1-7.1.9.1 A If a unique identification parameter is computed, the algorithm used shall meet the PCI DSS requirements concerning protection of card data.
- 1-7.1.9.2 A If the payment sequence is based on a unique identification parameter, the computation of this parameter shall neither require that the cardholder enters the PIN, nor that the cardholder is requested to enter the PIN.
- 1-7.1.9.3 A If entry of the correct PIN is not needed for further transaction processing, the cardholder shall not be prompted to enter his PIN, i.e. no display message requesting PIN entry shall appear.

1-7.2 Nets PA-DSS Implementation Guide

NOTE: The PSAM PA-DSS Implementation Guide is a separate document available to terminal manufacturers and vendors having an active development agreement with Nets Denmark A/S.

1-8 Basic Transaction Flow

1-8.1 The Four Steps

1-8.1.1 Introduction

When performing a payment transaction, e.g. a purchase, on a terminal conforming to this specification, the terminal uses the PSAM via what is basically an API.

The terminal uses four basic commands towards the PSAM to initiate and complete a transaction:

- Initiate Payment,
- Payment,
- Validate Data,
- Complete Payment.

When performing a chip card transaction, these four basic commands are called "Initiate EMV Payment", "EMV Payment", "Validate Data" and "Complete EMV Payment".

When performing a magnetic stripe based transaction, the four basic commands are called "Initiate MSC Payment", "MSC Payment", "Validate Data" and "Complete MSC Payment".

Key entered and token based transactions are also possible, while specialized transactions are available.

Two specialized transactions are possible. One is used to cancel an already completed transaction while the other is used to identify a token.

See also section 1-9, page 1-9-1, Best Practice.

Before any transaction processing can take place, application initialization have to take place. See section, 2-4.16 page 2-4-23, Terminal Initialization and section, 2-5.1 page 2-5-1, Application Initialization.

1-8.1.2 The Basic Commands

The basic transaction flow is described under the assumption that an attended terminal integrated with a cash register is used together with a chip card.

A transaction using a chip card is started by either a cardholder inserting the chip card in the chip card reader or by the merchant initiating a business function on the cash register.

When the cardholder inserts the chip card, application selection is initiated. The flow during application selection is described in ref.20: "EMV ICC Specification", in section 1-14.3 page 1-14-3, Application Selection and in section 2-3.3 page 2-3-8, Application Selection.

When application selection has been completed, the terminal shall send the first of the four commands to the PSAM. The amount does not need to be available before initiating the first command.

- 1-8.1.2.1 C Before issuing any *Initiate Payment* command, the terminal may validate whether the Business Call (initiated by the merchant) is supported by the PSAM for the AID in question or not. This is done by validating the two data elements:
- Card Product Type (Debit, Credit, Prepaid etc.)
 - Card Product Functions (Purchase, Refund etc.)
- NOTE:** Card Product Type and Card Product Functions can for PSAM based terminals be obtained by issuing a *Get D/C Properties* command to the PSAM with Identifier = '0009'.
- 1-8.1.2.2 C If the Business Call can not be processed due to limitations in the data elements listed above, the terminal may display "Invalid transaction" (Message Code = 'FF').
- NOTE:** The requirements 1-8.1.2.1 and 1-8.1.2.2 are applicable for ICC transactions (Debit, Credit or Prepaid) only.
- 1-8.1.2.3 A The transmission flow shall only be controlled by the ASW's returned from the PSAM. The terminal shall itself **not** change the flow due to missing host response a.s.o.

Initiate Payment

This first command from the terminal provides the PSAM with the following central data:

- The transaction amount,
- Which type of card data input is used,
- The date and time,
- Under which circumstances the transaction is prepared (see section 2-13.9.5 page 2-13-70, POS Entry Mode),
- Which type of transaction is called for (see EMV for Transaction Type).

If PIN is used as cardholder verification method (CVM), the PSAM itself attains the PIN from the PIN Pad in the user interface.

If the amount is present in the Initiate Payment command, Early Amount Entry is performed. If the amount is not present in this command, the PSAM will prompt for it when required. In this case, Late Amount Entry is performed.

Payment

After receiving this second command, the PSAM asks the terminal for check against possible/voluntary stop list and possible approval code attained by the merchant before the transaction was initiated. The terminal also delivers additional data to the PSAM which are to be used during reconciliation. Data like a batch number during reconciliation.

The response from the PSAM to the terminal on this second command may contain a request to be sent online.

Validate Data

This third command is used to deliver the response from the acquirer, if any, concerning the request sent in connection with the payment command to the PSAM.

The PSAM returns the action code and the system trace audit number to the terminal.

Complete Payment

In this final command, the terminal communicates the final status of the transaction, as seen by the terminal, to the PSAM. For example, if the cardholder verification method used is signature and verification of the signature is used, the terminal tells the PSAM whether the cardholder signature was accepted by the merchant.

In the response to the complete command, the PSAM communicates the final result of the transaction. If the transaction initiated was an authorization, a token may also be returned to the terminal.

Transaction flow

The general transaction flow is outlined in figure 1-8.1, Basic Transaction Flow. For details on the transaction flow, see e.g. chapter 2-5, Debit/Credit Functionality.

NOTE: Please notice that e.g. "Initiate X Payment" represents e.g. "Initiate EMV Payment", "Initiate Key Entered Payment" etc.

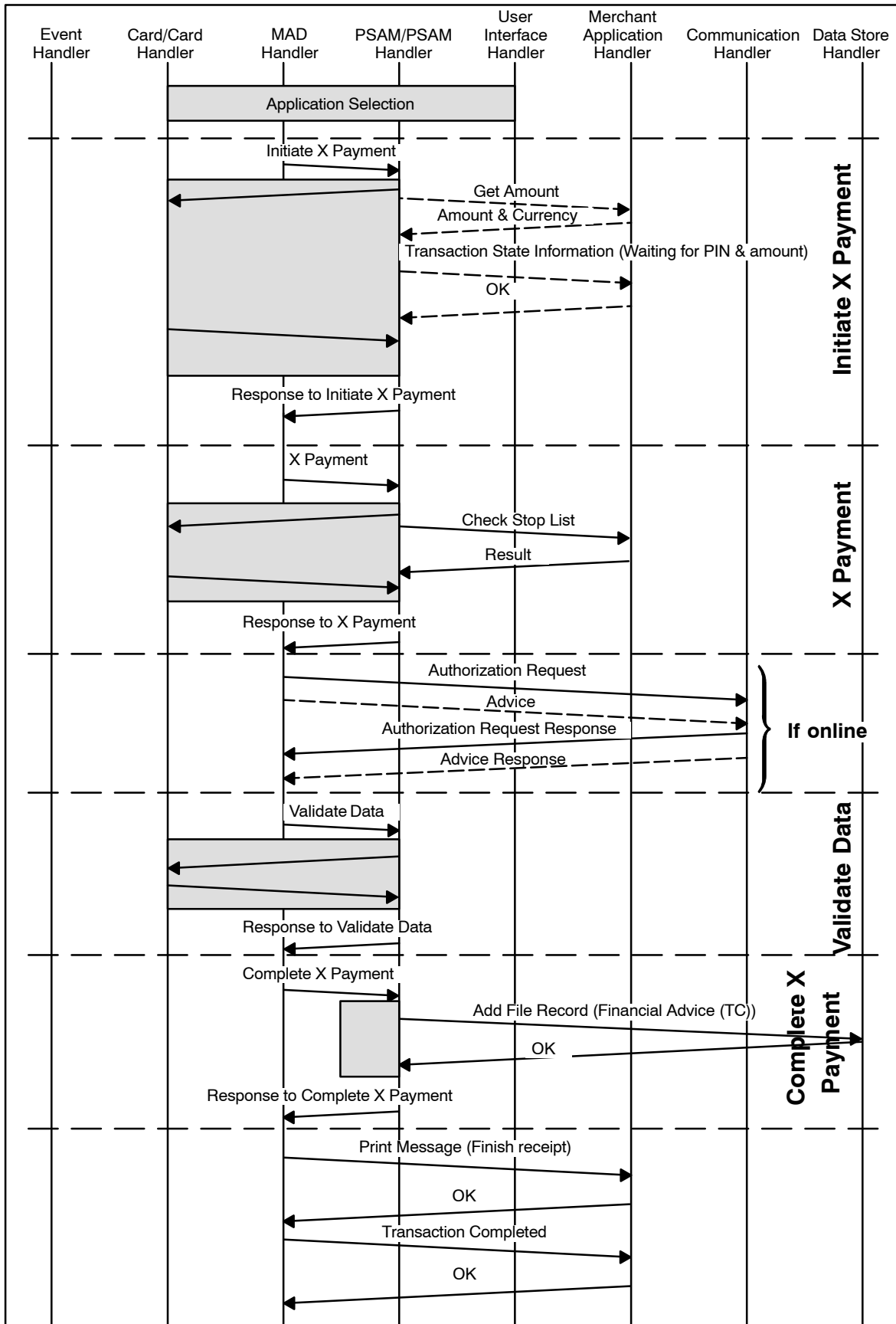


Figure 1-8.1 - Basic Transaction Flow

1-9 Best Practice

1-9.1 Introduction

The purpose of this chapter is to list a number of useful hints and guidelines for both terminal developers and developers of cash register systems interfacing PSAM based terminals.

Although this chapter is an integrated part of the "Technical Reference Guide - Open Terminal Requirement Specification", it may be seen as a separate description or summary of items worth paying special attention.

This chapter is informative. There is, in most of the sections, a reference to the other sections in the OTRS, where additional information and specific requirements can be found.

1-9.2 Documentation

For both stand-alone terminals and implementations where the terminal is connected to a cash register system, a user manual for the terminal shall be provided.

This manual shall contain sufficient information making the staff able to operate the system concerning card payments and settlements. For stand-alone terminals, the terminal supplier supplies the manual while the system supplier is expected to deliver the manual for terminals connected to a cash register.

The manual shall also contain relevant technical information, including guidelines for PSAM replacement.

1-9.3 Terminal Categories

The design of a terminal shall consider the environment in which the terminal is intended to operate. The terminal may either be designed to operate in a 'normal' attended shop-environment, or to operate in an unattended self-service environment.

A terminal must be designed to operate according to one (or more) of the following categories:

- Attended - with PIN Entry Device
- Unattended - with PIN Entry Device
- Unattended - without PIN Entry Device

The terminal shall be able to present parameters showing the Terminal configuration. The parameters may e.g. be presented as a Terminal Report.

1-9.4 Choice of Business Call

Each time a new transaction (or a sequence of transactions) is initiated, a Business Call is required.

Seven different Business Calls have been defined, and the use of these calls depends on the actual business situation.

If the final transaction amount is known when the transaction is initiated, the two Business Calls

- "Purchase"
- "Refund" (in case of credit transactions)

can be used.

Concerning surcharges, please refer to section 1-9.19 page 1-9-13, Addition of Surcharges and Fees.

If only an estimated amount is available when the transaction sequence is initiated, the Token based Business Calls can be used:

- "Original Authorization",
- "Extended Authorization",
- "Supplementary Authorization",
- "Capture" and
- "Reversal (Authorization)"
- "Post Purchase"
- "Post Refund"

Depending on the business environment, the amount to be authorized shall be agreed upon with the individual acquirers.

Support of Supplementary Authorization depends on the individual card schemes.

If a transaction needs to be cancelled, this can be done under specific conditions by using the Business Call

- Cancellation

If the conditions cannot be met, a Refund may be used in order to return funds to the cardholder.

References

Business Calls, definition: Section 1-10.2 page 1-10-2, Calls to the PSAM.

Concerning Refund

When a Refund transaction is going to be performed and the card contains several applications, the merchant shall (in a dialogue with the cardholder) decide which application to use.

Refund transactions are not applicable for unattended terminals and attended terminals performing cash transactions.

The CVM selected for Refund transactions is always Signature. Unlike normal Purchase transactions, it is the merchant who shall sign the receipt handed over to the cardholder.

Cashback is not applicable for Refund transactions.

References

Refund: section 1-10.2.6 on page 1-10-6.

1-9.5 Support of Card Technologies

Four different Card Data Sources (or card technologies) have been defined:

- ICC,
- Magnetic Stripe (Track 2 or Track 3)
- Key-Entered and
- Contactless (ICC and MSD)

A terminal able to accept Debit/Credit cards shall accept both ICC and Magnetic Stripe (including fallback from ICC) as card data source.

References

Card Data Source, definition: Section 2-15.2.26 on page 2-15-7.

1-9.6 ICC Technology and Fallback to Magnetic Stripe

When an ICC is inserted into the ICC reader, the terminal shall try to communicate with the ICC. This communication may fail, and fallback from ICC to Magnetic Stripe may be the only way to continue and complete the transaction.

If the terminal is attended and the terminal has separate ICC and Magnetic stripe readers, the merchant shall be able to testify that the ICC has been inserted correctly, before fallback to magnetic stripe may continue.

To be able to testify correct card entry, the Merchant Interface shall include two keys/menu items (“Yes”/“No”) to activate when the question “Card inserted correctly?” appears.

If the magnetic stripe is used and the magnetic stripe indicates that the card contains an IC, the terminal shall reject the attempt and request the cardholder to use the ICC reader instead.

A transaction based on Fallback may be rejected by the issuer.

References

Fallback, description: Section 2-4.17, Fallback from Chip (ICC) to Magnetic Stripe (MSC) on page 2-4-24.

Card inserted correctly: Section 2-4.17.2 on page 2-4-24.

1-9.7 Service Packs

In order to add new variants of existing commands and responses, the term Service Pack is used.

In order to be able to utilize the new variants as defined by a Service Pack, it is essential that both the terminal and the PSAM supports the Service Pack.

A function has been defined, which makes it possible for the terminal to decide the highest level of Service Packs supported by both entities.

A terminal designed according to this specification supports at least Service Pack 2.

References

Service Packs: Section 2-5.1.3, Restart page 2-5-6

Service Packs: Section 2-8, Service Packs page 2-8-1

1-9.8 Application Selection

When an ICC card is inserted in the terminal, the terminal builds the Candidate List. The Candidate List is the list of applications supported by both the actual ICC card and the terminal. The Candidate List may contain:

- No matching applications (i.e. the list is empty)
- One matching application
- More than one matching application.

If more than one matching application is found, the cardholder shall decide which application to be used. This selection shall be performed as a dialog between the cardholder and the terminal. The Merchant Interface may display to the merchant that an application selection or application acceptance is in progress and the cardholder action is awaited. The information displayed may include the application candidate(s).

If a Refund transaction is initiated, it is either the merchant or cardholder who shall decide the application to be used (if more matching applications have been identified). This may be implemented as a dialogue box (showing the Candidate List) on the Merchant Interface.

NOTE: Country specific requirements may exist.

References

Application Selection: Section 1-14.3, Application Selection on page 1-14-3.

Please take special note of section 1-14.3.4 page 1-14-11, MSC Application Selection and in particular requirement 1-14.3.4.4 page 1-14-12.

1-9.9 Support of Cardholder Verification Methods

The CVM (Cardholder Verification Method) to be used is decided by the PSAM. Based on the PSAM configuration, the

Terminal Capabilities and data from the actual card, the PSAM will decide the actual CVM. That means that at the time of transaction initialization, the terminal will not know whether

- PIN,
- Signature,
- No CVM
- Combined CVM (a combination of PIN and signature)

is going to be selected.

Default transactions shall be initialized without requesting any specific CVM, thus leaving the choice to the PSAM and card.

If the terminal is “attended”, the terminal (incl. Merchant Interface) shall be able to support all the possible CVMs defined:

- PIN (online PIN or offline PIN verification),
- Signature,
- Combined CVM (offline PIN and Signature) and
- No CVM.

If the terminal is “unattended”, the use of Signature as CVM is not relevant. Whether PIN is relevant or not, depends on whether a PIN Entry Device is present or not.

Some card schemes accept that the cardholder does not remember the PIN, even though these cards are expected to generate PIN-based transactions.

To be able to support such customers, the Merchant Interface shall include a key/menu item to be activated when Signature shall be used instead of the CVM otherwise decided by the PSAM. The function to request a specific CVM is called “Forced CVM”.

The Merchant Interface may also include a key/menu item to give PIN priority as CVM.

The data element Merchant Initiative (bits 1, 2 and 8) is used to convey the request for a specific CVM to be used.

Whether the request for a specific CVM will be accepted or not, depends (among others) on the PSAM parameters and the actual card.

References

Forced CVM: section 2-9, Merchant Initiative Bypass page 2-9-1.

Merchant Initiative, definition: Section 2-15.2.93 on page 2-15-24.

1-9.10 Temporary Offline Procedure

Card processing performed by the PSAM may imply that an online request shall be performed. If the terminal is not able to communicate with the host systems temporarily, e.g. due to technical problems in the communication network, the transaction (normally) fails. The ASW1-ASW2 = '1618' (No host data received), received from the PSAM indicates that no host response is received.

If the terminal is not able to communicate with the host systems, the merchant may be able to initiate a transaction using a Temporary Offline Procedure. This procedure will indicate to the PSAM that the transaction processing shall be performed offline, i.e. without initiating an online request. Whether the procedure will be completed successfully or not, depends on the configuration of both the PSAM and the actual card. The function, to request a transaction to be performed offline, is called "Forced Offline".

To be able to use the Temporary Offline Procedure the Merchant Interface shall include a key/menu item to be activated when offline processing is requested.

The Merchant Interface may also include a key/menu item to request online processing.

The data element Merchant Initiative (bits 5, 6 and 7) is used to convey the request for specific online/offline processing. Request for the Temporary Offline Procedure is indicated by the value '60' in Merchant Initiative.

When the merchant initiates the Temporary Offline Procedure the guarantee limit may differ from the general rules. The individual acquiring agreements, signed by the merchant and the acquirers, define the consequences.

If the merchant obtains an Approval Code, e.g. by making a phone call to acquirer's helpdesk, this may to some degree compensate for the reduced guarantee.

How to obtain an Approval Code in case of temporary offline is described in section 1-9.11 page 1-9-6.

References

Merchant Initiative, definition: Section 2-15.2.93 on page 2-15-24.

1-9.11 Voice Authorization Calls

If the 'Temporary Offline Procedure' has been requested by the merchant, the merchant should be requested to make a manual Voice Authorization Call.

A Voice Authorization Call may be performed by calling the card issuers helpdesk (or voice response equipment) for an Approval Code. The Approval Code consists of max. 6 alphanumeric characters.

The request for Voice Authorization Calls may be combined with or replaced by a manual look up in a Stop List (specific requirements may depend on the agreements between the merchant and the acquirer(s)).

The response to the request for a Voice Authorization Call may either be:

- No Voice Authorization Call Performed,
- No Voice Authorization Call Performed, but the card number is found in the Stop List.
- Voice Authorization Call performed, but the authorization request has been declined,

- Voice Authorization Call performed, and the authorization request has been approved.

If the manual authorization request has been approved, an Approval Code has been received over the phone.

The merchant shall be able to select the appropriate response to the request, and if approved, be able to enter the Approval Code received.

The terminal solution may give the merchant the opportunity to switch off the request for a manual procedure. Instead of asking the merchant, an automatic answer (No Voice Authorization Call Performed) may be given.

In order to obtain a Voice Authorization, the PAN must be known. The expiry date and the CVV2 may also be needed. During the transaction, the PSAM/Terminal will inform the merchant about the actual PAN (to be provided in the *Check Stop List* command). This ensures that the PAN used originates from the correct application, especially in case of multi-application cards.

If the Voice Authorization Call is performed before the transaction is initiated, the PAN embossed on the card will be used. But in case of multi-application cards it may be impossible to visually read the PAN of the selected application.

References

Voice Authorization: Section 2-5.5.4 page 2-5-25, EMV Payment and section 2-5.7.4 page 2-5-47, MSC Payment.

1-9.12 Stop List

If the terminal supports offline transactions, a Stop List may be implemented.

Usually the Stop List will be stored on the merchant operated part of the terminal solution.

Updates to the Stop List, as well as a complete Stop List, shall be obtained directly from the acquirer by calling the dedicated platform for Stop List information.

Nets Denmark A/S does not support the use of Stop List's.

During transaction processing the PSAM will request a look up on the Stop List in the following situation:

- If the transaction is processed offline (both MSC and EMV cards), e.g. due to requesting the 'Temporary Offline Procedure'.

The response to the request for look up on the Stop List depends on whether:

- No Stop List is available,
- Stop List is available, but the actual card number is not found in the list, or
- Stop List is available, and the actual card number is found in the list

If the actual card number is found in the Stop List, the list may indicate whether the card shall be picked-up (if possible).

References

Check Stop List command: Section 2-14.6.19 on page 2-14-97.

1-9.13 Optimizing the Transaction Time

1-9.13.1 Parallel Processing

In general, the overall transaction time may be reduced if more tasks are performed in parallel. As an example, printing may be started before the entire content is known and ICC data may be read by the terminal/PSAM while the merchant calculates the transaction amount.

Accelerated PIN Entry

An example of parallel processing is that the cardholder may be prompted for PIN entry at an earlier point of time in the chip-based transaction when compared to a straight-forward implementation.

Two different variants of “Accelerated PIN Entry” have been implemented in the PSAM in order to speed up most transactions:

- APE, where PIN entry is requested after reading card data)
- DAPE (Dankort APE), where PIN entry is requested immediately after final application selection.

Terminals shall be able to handle the command flow depicted in table 2-5.3 page 2-5-30, which is fully in line with the TAPA architecture.

Release of the ICC

The terminal may release the card before the actual approval or denial of the transaction. The rules given in section 2-5.6.3 page 2-5-31, Release of the ICC shall be followed.

In this way, the cardholder can take the card in parallel with receipt printing.

1-9.13.2 Start before amount is known

It may, to speed up the processing, be desirable to start a transaction before the amount is known.

Get Amount 3

The terminal will in this case start the transaction with a zero amount. The *Get Amount 3* command, issued by the PSAM, will then request the amount from the Terminal/Cash Register.

The PAN may be unknown at this time (when the ICC card request the amount). The PAN will not be available in the

command, in this situation, the LEN_{PAN} will be equal to '00' and the data element "Amount Request" will indicate "Initial Amount" It is then up to the terminal/Cash register System to return either an estimated amount or an accurate amount.

If an estimated amount is returned, the PSAM will issue a subsequent *Get Amount 3* command requesting an accurate amount.

NOTE: The amount returned by the terminal to the command must be a non-zero value. This is a EMV requirement.

References

Get Amount 3 command: Section 2-8.5.1 page 2-8-5, *Get Amount 3*.

1-9.13.3 Data Transmission

Clock Frequency

For both the ICC and PSAM interfaces, it is recommended to use the maximum allowed clock frequency of 5 MHz. Although the internal computation is normally based on a clock signal generated internally in the ICC/PSAM, using the highest possible external clock frequency will lead to the fastest possible communication rate.

I/O Buffer Sizes for T=0 (ICC interface)

The terminal's I/O buffer should have sufficient length to avoid switching into single byte transmission (by use of procedure byte '60') when conveying large messages.

I/O Buffer Sizes for T=1 (ICC and PSAM interfaces)

The terminal's I/O buffers should have sufficient length to avoid chaining at the T=1 level. The maximum possible length of 254 bytes is highly recommended, especially at the PSAM interface.

Transmission Speed (ICC interface)

As required in ref. 20, "EMV ICC Specification" the terminal must support the values 1, 2 and 4 for the protocol parameter D (bit rate adjustment factor). In this way, the terminal will make use of the fastest possible data transmission supported by the ICC. The proposed communication parameters may be rejected by the terminal by use of a warm reset, resulting in the card returning to basic parameters supported by all terminals.

Transmission Speed (PSAM interface)

Transmission of data to and from the PSAM should take place at the highest possible transmission speed as relatively much data has to be exchanged. Therefore, the terminal should use PPS to select the highest possible speed supported by the

terminal. If the PPS is unsuccessful, the terminal should continue proposing the next lower speeds until the PPS negotiation is successful.

The current PSAM platforms all support the following parameter sets:

- F = 372, D = 1
- F = 372, D = 2
- F = 372, D = 4
- F = 372, D = 12

Future PSAMs may support additional parameter sets, such as:

- F = 372, D = 20
- F = 372, D = 32

References

Section 2-5.6, Optimizing the Transaction Time on page 2-5-29.

1-9.14 Signature Verification and Accept

When signature is selected as CVM, the merchant may be requested to compare the cardholder's signature (just written on the receipt) with the reference signature on the card.

The configuration of the PSAM defines whether the question shall be asked to the merchant or not.

The terminal supplier may decide to permanently request signature verification to be performed, irrespective of the PSAM configuration.

To be able to accept or reject the cardholder's signature, the Merchant Interface shall include a pair of keys (Yes/No) to activate when the question "Signature accepted?" appears.

The CVM selected for Refund transactions is always Signature. Unlike normal Purchase transactions, it is the merchant who shall sign the receipt handed over to the cardholder.

References

Signature Verification: Section 2-4.4.2, Signature on page 2-4-5.

1-9.15 Receipts

The requirements state that the cardholder shall be able to get a receipt when that cardholder has accepted the transaction.

If the transaction is PIN based the cardholder accepts the transaction by entering the PIN and accepting the amount (by activating the Enter key).

Since the cardholder accepts the transaction before the transaction result is known, a receipt shall be issued irrespective of the transaction result.

When PIN is used as CVM, the transaction may be rejected due to wrong PIN, and the cardholder will be requested to re-enter the PIN. If it is a magstripe transaction, the flow may continue after the PIN has been re-entered.

If the PIN has been online validated, a receipt shall be printed for each PIN entry.

If the PIN was offline validated and re-entered (early in the transaction sequence) the terminal must print at least one receipt (covering all PIN entry attempts).

If the transaction is signature based, the cardholder accepts the transaction by signing the receipt.

When a transaction is signature based, two receipts shall be printed. One to be signed by the cardholder and kept by the merchant, and one to be handed over to the cardholder.

If the function Signature Validation is enabled, and the merchant rejects the signature written, a receipt indicating that the transaction is rejected/cancelled due to "Signature Rejected" shall be printed and handed over to the cardholder. Consequently, the cardholder receipt can only be printed after the question "Signature accepted?" has been acted upon.

If the transaction is completed with No CVM (neither PIN nor signature), the cardholder (normally) accepts the transaction by accepting the amount. The cardholder just activates the Enter key when the amount appears in the display.

The cardholder shall get a receipt for each acceptance of the amount.

The terminal may, in an attended environment print receipts and similar informative text in case of errors, rejections, cancellation, etc., even though a receipt is not required. The printing must not interfere with the ordinary transaction processing.

References

Receipts: chapter 1-12 page 1-12-1, Receipts.

1-9.16 Transaction Result

During the processing of a transaction, the terminal shall send 4 commands to the PSAM.

The 4 commands are:

- *Initiate Payment* command,
- *Payment* command,
- *Validate Data* command and
- *Complete Payment* command

Even though the receipt data may be available after the *Validate Data* command has been processed, the final transaction result will not be known until the response from the *Complete Payment* command is received from the PSAM.

NOTE: Not only the ASW1-ASW2 value '0000' returned from the PSAM indicates approved/successful. Also

ASW values in the range '10XX' indicate approved/successful as defined in table 2-14.141 on page 2-14-131.

When a terminal is interfaced to a cash register system or a similar equipment, it is very important that the design of the communication between the individual devices (i.e. protocol, message formats etc.) consider that communication problems may occur. A mechanism shall be built-in to overcome such problems and to ensure (among others) that the final transaction result is distributed to all relevant entities.

References

Transaction result: Section 2-5.16.1 page 2-5-115, General Rules and section 2-14.10 page 2-14-130, ASW1-ASW2 Coding.

1-9.17 Transaction Checks

The PSAM offer two different features to avoid situations where a cardholder pays twice for the same goods.

Duplicate Transaction Check (PSAM)

The PSAM is able to validate when a new transaction is identical to the last transaction completed successfully by the PSAM.

The PSAM will see a new transaction as identical to a previous transaction, if all the following conditions are fulfilled:

- The PAN and PAN Sequence Number are identical
- The amounts and currencies are identical
- The same type of Business Call is used (Purchase, Refund, Post Purchase, Post Refund or Capture)
- No other transaction (of type Purchase, refund or Capture) has completed successfully since the first transaction
- The time between the two transactions is less than a specified time-out value.

If the new transaction is identified as identical to the previous, the new transaction will be rejected by the PSAM (ASW1-ASW2 = '1300' (Match on previous transaction)).

The default time-out value in which the check is active is 10 minutes.

Depending on the actual terminal environment, the terminal may modify the time-out value or disable the check. In environments where the same amount (and card) typical are used in consecutive transactions (e.g. ticketing machines), the check should be disabled!

Status of Previous Transactions (Terminal)

In excess of the control performed by the PSAM, the PSAM also offers a feature where the terminal and/or cash register system can request the status of a previously performed transaction having financial impact.

NOTE: A limited number of transactions are buffered for this check (typical 8 transactions).

References

Section 1-10.7 page 1-10-29, Status of Previous Transactions.

1-9.18 Cashback Amount

The merchant may, depending on the agreements with the acquirer, disburse a cash amount (cashback) as a supplement to the amount for goods or services.

If the cashback function is implemented, the amount for cash should be included in the transaction amount transferred to the PSAM. The amount for cash should be indicated in the data element Amount Other as a subset of the transaction amount.

A cashback shall be indicated using the same Currency Code as used for the total transaction amount.

It is not allowed to combined DCC and cashback.

When Cashback is indicated in Amount Other, the Transaction Type (TT) shall be set accordingly to '09' (Goods and services with cash disbursement).

References

Cashback, definition: Section 2-15.2.12 page 2-15-4, Amount, Other.

1-9.19 Addition of Surcharges and Fees

The merchant (or if automatically, the Cash Register) may add surcharges or other fees to the amount summed up for the goods or services.

Surcharges or fees shall be added before the transaction amount is determined and transferred to the PSAM. When the cardholder accepts a transaction, e.g. by entering the PIN or signing a receipt, the total amount shown shall include surcharges and other fees.

References

Surcharges and Fees: Section 1-10.15 page 1-10-97, Transactions with Tips/Gratuity.

1-9.20 Gratuity

In certain environments the cardholder may add gratuity/tips to the amount summed up for the goods or services.

Just as for surcharges and fees, the total amount displayed during PIN entry shall include any gratuity, i.e. the gratuity amount shall be agreed before PIN entry.

If the transaction is signature based, the receipt may contain space for the cardholder to add the gratuity.

References

Surcharges and Fees: Section 1-10.15 page 1-10-97, Transactions with Tips/Gratuity.

1-9.21 Dual Communication Access Points

During the processing of a transaction, the PSAM may initiate an online request to be executed, before the transaction processing is able to complete. To be able to execute the online request, the terminal shall be able to establish a connection to the host systems.

If the merchant initiates any of the administrative functions, e.g. Advice Transfer Request, a connection to the host systems shall be established too.

Irrespective of the background for establishing a connection to the host systems, the request for connection shall be performed identical.

To be able to offer the highest level of availability, Nets Denmark A/S has established two identical platforms. Each platform has its own set of communication lines to the external networks. Both platforms are active 24 hours per day.

Each platform has its own unique address. If a switched communication network is used (e.g. PSTN or ISDN), the two platforms shall be called using different numbers. The two platforms are also identified by individual IP-addresses.

To be able to utilize the high availability, utilized by the dual host platforms, the terminals shall be able to initiate a connection to the second platform, if a request for connect fails while trying to connect to the first platform.

The algorithm used to select which platform to call first, shall consider an equal load on both platforms in normal situations, and the algorithm shall also provide the necessary functionality to handle situations when one of the platforms is out of service.

References

Terminal Operator Communication Access Points: section 2-5.14.5 page 2-5-100 and Dual access points: Section 2-13.3 page 2-13-2, Communication Protocols.

See also chapter 2-5.14, Online Transaction and chapter 2-5.15, Transferring Advices.

1-9.22 Balancing and the Transfer of Advices

The transfer of advices is automatically controlled by the terminal, see chapter 2-5.15 page 2-5-101, Transferring Advices. However, just transferring advices does not in itself initiate a balancing. In order to perform balancing, an Advice Transfer must be initiated.

For attended terminals an Advice Transfer is normally initiated by the merchant or as a result of an action performed by the merchant.

An Advice Transfer shall be initiated frequently, and at least once a day. An Advice Transfer initiated by the merchant is usually followed by a PSAM Update sequence to ensure that the PSAM contains the latest configuration parameters.

Since no merchant is present at unattended terminals, the Advice Transfer and PSAM Update sequences shall be initiated automatically.

References

Transferring Advices: Section 2-5.15 page 2-5-101.

1-9.23 Log and Totals

The transaction log is not only relevant for audit purposes and technical trouble-shooting, but also for settlement purposes and for generating total reports.

Generally transaction messages may be divided into two main groups:

- Messages with no financial impact and
- Messages with financial impact.

Messages with no financial impact include (among other messages) Authorization Request messages, which may cause changes in the cardholders available amount limits, but no change on the account.

Messages with financial impact include (among other messages) Reversals, which may cause that an already registered message with financial impact shall be cancelled.

While messages with financial impact are stored locally in the terminal's Data Store, they will not be able to cause any changes on the cardholder's, nor the merchant's account. When a message with financial impact is transferred from the terminal to the acquirer, the response to the terminal will include information relevant for the total reports generated by the terminal. The response data includes the card name and card group for totals, and an indication of the actual settlement period.

Total reports shall be based on the messages with financial impact transferred from the terminal to the acquirer, but the report may also reflect messages not yet transferred.

References

Log: section 1-14.10 page 1-14-24, Log, and section 1-9.25.6 page 1-9-25, Total Reports and section 1-9.25 page 1-9-16, Guidelines for Construction Total Reports.

1-9.24 Merchant Application Log

The Data Store in a terminal is used to store messages temporarily until they can be transferred to the host systems. All messages stored in the Data Store are generated by the PSAM.

The PSAM offers a function for automatic generation of a back-up of the Data Store. This back-up is directed to the merchant's side of the terminal equipment, e.g. in the cash register system. The Data Store back-up (or Merchant Application Log) receives a copy of all messages sent to the normal Data Store.

If the Data Store becomes defective, the messages stored in the Merchant Application Log may be used as back-up messages, and these messages may be delivered instead of the messages lost in the terminal's Data Store.

The terminal defines by the data element Info Level (bit 1) whether the PSAM shall store messages in the 'normal' Data Store only, or in both the Data Store and the Merchant Application Log.

References

Logging: Section 2-5.1.3, Restart on page 2-5-6.

1-9.25 Guidelines for Constructing Total Reports

1-9.25.1 Introduction

During the development of terminal implementations, some guidelines or examples concerning how to design the Total Reports may be helpful.

This section explains the principles for the design of Total Reports and the principles for sorting the data presented by the Reports.

1-9.25.2 General

Generally the terminal shall be able to generate a Total Report. This report shall include the data necessary for the merchant to perform an appropriate balancing between the terminal and the settlement statements generated by the acquirers.

There are no standard way for construction of the total report. How and when individual transactions and/or a batch of transactions are settled is dependant upon the contracts agreed between the merchant and the acquirer(s).

The terminal operator is not involved other than 'collecting' the transactions and routing these appropriately.

The only requirement stated by the terminal operator in this connection, tells that the Total Report printed must be useful

for determining which transactions were accepted for further processing and when these were reconciled.

The report must also include information which makes the merchant able to match individual transactions and/or a 'batches' of transactions on the total report with a 'settlement' printout received from the acquirers.

1-9.25.3 Data Elements

In order to assist when building the Total Report a number of data elements are defined:

Table 1-9.1 - Total Reports - Related Data Elements

Data Elements	APACS Field
Batch Number	37
Card Reconciliation Counter ID	44
Card Reconciliation Counter Name	44
Date Reconciliation	28
Reconciliation Indicator	29
Date, local transaction	12
Time, local transaction	13

Batch Number

The Batch Number is usually used by the acquirer to identify a batch of transactions. The data element may be included in the 'settlement' printout the acquirer periodically make available to the merchant.

The value of the data element Batch Number is assigned by the merchant and/or the terminal equipment.

Card Reconciliation Counter Id- and Name

The Card Reconciliation Counter Id and Card Reconciliation Counter Name is assigned by the terminal operator to help the merchant (and the terminal equipment) to identify which 'group' of payment cards individual transactions adheres to. The data elements may be used in the 'settlement' printout.

The value of the data elements Card Reconciliation Counter Id and Card Reconciliation Counter Name are received in the response to Financial Request- and advice messages, incl. financial reversal messages.

Date Reconciliation

The Date Reconciliation is used to determine when a transaction is reconciled, i.e. recorded (not settled) at the acquirer. The data element may be used in the 'settlement' printout.

The value of the data element Date Reconciliation is received in the response to Financial Request- and advice messages, incl. financial reversal messages.

Reconciliation Indicator

The Reconciliation Indicator is used to 'break down' a reconciliation period (Date Reconciliation) into several sub-peri-

ods. Acquirers may perform settlement processing several times during the day. This data element may indicate the sub-period assigned to the individual messages, and may be used by the acquirers in the 'settlement' printout.

The value of the data element Reconciliation Indicator is received in the response to Financial Request- and advice messages, incl. financial reversal messages.

Date, local transaction and Time, local transaction

The two data elements Date, local transaction and Time, local transaction may also be used by the acquirer to identify transactions on the 'settlement' printout.

Reference

See section 2-4.18 page 2-4-34, Counters and Batch Numbers.

1-9.25.4 Example

Below is given an example of how some of the (relevant) data elements could be used to make a Total Report.

It is assumed that the merchant and the acquirers has entered into an agreement in which the following data elements/information is used in the 'settlement' statement provided by the acquirer(s):

- Batch Number,
- Card Reconciliation Counter Id and -Name,
- Reconciliation Date and,
- Reconciliation Indicator.

It is also assumed that the merchant accept:

- Dankort,
- MasterCard and
- Diners.

The transactions are bundled in batches by the terminal.

Each batch created is identified by the data element Batch Number.

The Batch Number is assigned by the terminal equipment (or the merchant).

A batch must only contain transactions in one currency.

The transactions in each batch is divided into 'settlement groups' identified by the data elements: Card Reconciliation Counter Id and Card Reconciliation Counter Name.

Transactions made using e.g. a Dankort is placed under the 'Dankort' Card Reconciliation Counter Id.

It shall be noted that Financial Advices does not have a Card Reconciliation Counter Id attached before the advice has been sent to the terminal operator and the response has been received, i.e. the value is extracted from the advice response.

This means that the total report can only be made *after* all advices have been transferred (i.e. an Advice Transfer has taken place).

Table 1-9.2 - Report Segmentation (Example)

Batch Number	Card Reconciliation Counter ID (and Name)	Reconciliation Date	Reconciliation Indicator
1	C01 (DANKORT)	020120	000
		020121	000
	C03 (MASTERCARD)	020121	001
			002
			003
			004
		020122	001
			002
	C05 (DINERS)	020122	001
			002
2	C03 (MASTERCARD)	020121	001
			002
			003
			004
		020122	001
	C05 (DINERS)	020122	002

Each (financial) transaction is given a Reconciliation Date (Financial Advices when they are sent to the terminal operator).

This determines when the transaction is registered at the Acquirer, not when the transaction is settled. The actual settlement date is determined by the agreement between the merchant and the acquirers.

Each transaction has a Reconciliation Indicator attached (Financial Advices when they are sent to the terminal operator) with which the acquirers may split up the Reconciliation Date in several periods.

Each transaction can, in the Total Report, be identified and grouped together by:

- Batch Number,
- Card Reconciliation Counter Id (and Name),
- Reconciliation Date and
- Reconciliation Indicator.

To enable the merchant to balance totals counted by the cash register with the Total Report generated by the terminal equipment, the Total Report may include a grand total for each batch (including all cards in the batch).

The requirements for the calculation of sub-totals in the Total Report may depend on the settlement agreements between the merchant and the acquirers.

Individual sub-totals may be calculated

- for each Card Reconciliation Counter Id,

- for each Reconciliation Date (per card type) and
- for each Reconciliation Indicator (per card type and date).

Depending on the demands defined by the merchant other sub-totals may be calculated.

1-9.25.5 Proposal for accumulating data for Totalling Reports

Generally a total report shall reflect the financial result of a well-defined period of time - and for the terminals such a well-defined period is identified by the Batch Number (or Batch Numbers) assigned for this period.

A total report shall be based on the transactions or Business Functions performed during the period, but not all Business Functions have financial impact.

E.g. some Business Functions generates only Authorization messages, which of course have relevance for both the Merchant and the cardholders, but no direct financial impact.

Therefore only transactions with financial impact needs to be included in totals reports.

The following table shows the connection between Business Functions (identified by the data element Transaction Request) and the impact in total reports.

Table 1-9.3 - Transaction Requests and Totals Affected

Transaction Request (TR)	Totals Effected
00 Purchase	YES
01 Refund	YES
02 Original Authorization	NO
03 Supplementary Authorization	NO
04 Capture	YES
05 Authorization, Reversal	NO
06 Cancellation	YES
07 Extended Authorization	NO
09 Extended Authorization 2	NO
0A Post Purchase	YES
0B Post Refund	YES

Transaction Record - a way to accumulate Totals

To be able to generate suitable total reports the data related to all transactions with financial impact may be saved in e.g. a data structure as defined below.

The present proposal may only be seen as an example. This example has been defined with the aim of explaining the mechanisms for the accumulation of data for the total reports. In the present example the data structure is named a Transaction Record.

Depending on the specific terminal architecture, other principles or implementations may be more 'convenient'. A functionality for log- and data accumulation may be combined.

Table 1-9.4 - A Proposal for Transaction Record Layout

Data Element	Value		
Transaction Request (TR)			
Transaction Type (TT)			
Amount – transaction			
(Cashback Amount)			
Currency Code			
Batch Number			
Transaction Result (OK/Not OK)			
Reference STAN		Recon. Date	Recon. Indicator
STAN 0206 Message			
STAN 0226 Message			
STAN 0426 Message (02x6)			
Card Reconciliation Counter ID			
Card Reconciliation Name			
(Card Name)			
(Thread ID)			
(Card Data Source)			
(CVM Status)			

From the Transaction Request is initiated until the final transaction result is known, the PSAM should have generated one or two of the following message types (with financial impact):

- Financial Request (0206 message)
- Financial Advice (0226 message)
- Reversal Advice (0426 message)

The Transaction Record includes individual data elements for the identification of these message types:

STAN 0206 Message
 STAN 0226 Message
 STAN 0426 Message (02x6)

When these data elements are filled in, the value shall be set to the 'Systems Trace Audit Number' from the actual APACS message header (tag 'C4').

Not all combinations of 'filled in' or 'empty' for these three data elements are relevant, like the legal combinations depends on whether the Transaction Result indicates 'OK' (completed successfully) or 'not OK'.

Since each message is identified by a unique value for the STAN, the notation "Reference STAN" has been introduced.

The Reference STAN is used to link all messages related to a single Transaction Request.

Advices with financial impact will include the Reference STAN as tag 'D1' in the APACS message header.

Financial Requests will include the value of the Reference STAN directly in tag 'C4'.

The identification of advices with financial impact may be filled into the Transaction Record:

- when the advices are transferred from the PSAM to the Data Store,
- after the advices are saved in Data Store, but before transfer from Data Store to host system, or
- when the advices are transferred from Data Store to the host system.

If the terminal/MAD-Handler needs an overview of the advices present in the Data Store, the terminal/MAD-Handler may at any time read all the messages in Data Store, to identify advices with financial impact.

Initialization

Each time a new transaction with financial impact (Purchase, Refund or Capture) is initiated, a new Transaction Record is 'reserved' and the following data elements are filled in:

- Transaction Request TR,
- Transaction Type TT,
- Amount - transaction (when available),
- Cashback Amount (if relevant and when available),
- Currency Code
- Batch Number

The following data elements may be filled in with default/initial values like:

- Card Recon. Counter ID = 999
- Card Recon. Counter Name = "BETALINGSKORT"
- Card Name = "BETALINGSKORT" (if implemented)

If the terminal is implemented as a 'multi-thread implementation', the Thread ID assigned by the Mad-Handler may be a helpful information for identifying all messages generated during a specific Business Function.

The data element Card Data Source may also be relevant when total reports shall be generated.

All the other data elements shall at the time of initialization be filled in with a value indicating 'empty'.

In the response to the *Initiate Payment* command the PSAM will indicate the value for the data element STAN. This value shall be interpreted as the Reference STAN.

The Cardholder Verification Method may also be a relevant information. The data element CVM Status is available in the response to the *Payment* command.

If neither a Financial Request (0206) nor Financial Advice (0226) has been generated during the transaction flow, the transaction will have no financial impact and the Transaction Record may be 'released' again.

Data elements filled in during online requests

During the transaction sequence the terminal will be able to fill in data elements as these values become available.

If an online request is initiated, this request may either be an Authorization Request (0106-message) or a Financial Request (0206-message).

If a Financial Request is initiated the data element STAN 0206 Message shall be filled in (value selected from the APACS Message Header tag 'C4'), and the corresponding fields for reconciliation information may be filled in with default values like:

- Recon. Date = actual date in the format YYMMDD
- Recon. Indicator = 000

If a Financial Request response (0216-message) is received the following data elements shall be extracted from this message and filled into the Transaction Record:

- Recon. Date (for STAN 0206 Message),
- Recon. Indicator (for STAN 0206 Message),
- Card Recon. Counter ID,
- Card Recon. Counter Name and
- Card Name (if implemented)

If no Financial Request response is received, no data elements can be extracted and filled into the Transaction Record.

Data Elements filled in during Transaction Completion

During the 'completion section' of a transaction flow a Financial Advice (0226-message) or a Reversal Advice (0426-message) may be saved in the Data Store. In some error-situations both types of advices may be generated and saved.

If these advices have financial impact, the APACS header will include the Reference STAN in tag 'D1'.

If a Financial Advice (0226-message) is generated and saved in the Data Store, the data element STAN 0226 Message may be filled in (value selected from the APACS Message Header). The corresponding fields for reconciliation information should remain 'empty'.

If a Reversal Advice (0426-message) is generated and saved in the Data Store and either a Financial Request (0206-message) or a Financial Advice (0226-message) has been generated, then the data element STAN 0426 Message (02x6) may be filled in (value selected from the APACS Message Header). The corresponding fields for reconciliation information should remain 'empty'.

If a Reversal Advice (0426-message) is generated, but no Financial Request or Financial Advice have been generated in advance, the Reversal Advice will have no financial impact.

When the transaction sequence is completed, the terminal will know whether the transaction was completed successfully or not, and the last data element may be filled in:

- Transaction Result

As described in the section "Transaction Record - a way to accumulate Totals", the identification of advices with financial impact may be filled in the Transaction Record at the time when the advices are saved in Data Store or later on.

Data elements filled in during transfer of Advices

If any advices with financial impact have been generated during the transaction sequence, the final reconciliation information will not be known until these advices have been transferred.

When a positive response to an advice with financial impact is received (i.e. tag 'D1' and 'D2' were present in the APACS header of the advice), the following data elements shall be extracted from the response message and filled into the Transaction Record:

- Recon. Date (for STAN 0226 Message or STAN 0426 Message (02x6)),
- Recon. Indicator (for STAN 0226 Message or STAN 0426 Message (02x6)),
- Card Recon. Counter ID,
- Card Recon. Counter Name and
- Card Name (if implemented)

If a negative response to an advice is received, no data shall be extracted from the response.

Result - 'OK' or 'Not OK'

When the transaction sequence, including a transfer of advice(s), is completed, all information necessary for generating an adequate total report will be available.

If Transaction Result indicates 'OK' then 2 different situations may have occurred:

A1 An online Financial Request/Response sequence is completed successfully:

STAN 0206 Message	is filled in
STAN 0226 Message	is 'empty'
STAN 0426 Message (02x6)	is 'empty'

A2 A Financial Advice has been generated successfully either after an offline validation or after an online Authorization Request:

STAN 0206 Message	is 'empty'
STAN 0226 Message	is filled in
STAN 0426 Message (02x6)	is 'empty'

If Transaction Result indicates 'not OK' then 3 different situations may have occurred:

B1 The response to the original online Financial Request has been received, but the response indicated that the transaction was rejected:

STAN 0206 Message	is filled in
STAN 0226 Message	is 'empty'
STAN 0426 Message (02x6)	is 'empty'

B2 No acceptable response to the original online Financial Request is received:

STAN 0206 Message	is filled in
STAN 0226 Message	is 'empty'
STAN 0426 Message (02x6)	is filled in

B3 The transaction is not completed successfully even though a Financial Advice has been saved in Data Store (or sent to the Data Store):

STAN 0206 Message	is 'empty'
STAN 0226 Message	is filled in
STAN 0426 Message (02x6)	is filled in

Until the messages identified by the data elements STAN 0226 Message and STAN 0426 Message (02x6) have been transferred successfully, the corresponding fields defining the reconciliation information must remain 'empty'.

Result - Irrelevant or with no Financial Impact

The following 3 results have been included in this document for information purposes only.

- C1 No messages with financial impact (0206/0226) and no corresponding reversal (0426) has been generated:
 - STAN 0206 Message is 'empty'
 - STAN 0226 Message is 'empty'
 - STAN 0426 Message (02x6) is 'empty'
- C2 No messages with financial impact (0206/0226) but a corresponding reversal (0426) has been generated. This combination will have no financial impact:
 - STAN 0206 Message is 'empty'
 - STAN 0226 Message is 'empty'
 - STAN 0426 Message (02x6) is filled in
- C3 Both a Financial Request/Response (0206) and a Financial Advice (0226) has been completed successfully and a corresponding reversal (0426) may or may not have been generated. This combination is not valid:
 - STAN 0206 Message is filled in
 - STAN 0226 Message is filled in
 - STAN 0426 Message (02x6) is filled in or 'empty'

All these combinations should not occur according to the explanations stated in the previous sections.

1-9.25.6 Total Reports and DCC

Each transaction initiated shall belong to a Batch Number, according to this specification, see section 2-4.18 for further information.

The Batch Number is indicated to the PSAM in the *Payment* command. The terminal will therefore be aware whether the actual transaction is a DCC-transaction or a normal transaction, before the Batch Number is forwarded to the PSAM.

For DCC-transactions the settlement between the acquirer and the merchant is based on the total transaction amount in the merchants local currency (in Denmark DKK).

Since the merchant balance of DCC-transactions is based on the amount in the local currency, the total reports shall be based on these amounts too ("Amount (ME)").

Since all DCC-transactions irrespective of the cardholders billing currency are settled in the merchants local currency, all transactions may belong to a single Batch Number. Even the normal transactions performed in the merchants local currency may be included in the same Batch Number.

Whether all DCC transactions shall be seen as a single Batch Number or not, may depend on the merchant requirements and wishes.

Separating the DCC-transactions in batches depending on the cardholders billing currency may be helpful for the merchant during the balancing process.

Which additional totals and subtotals the terminal may count and show in total reports (e.g. surcharges, amount in cardholders currency, DCC commissions, Mark Up amounts, Gratuity etc.) may depend on the merchants requirements and wishes.

1-9.26 Host Messages

Each response from the host may contain additional information.

The Host has the possibility to request a PSAM Update (Tag 'C9').

How the terminal reacts to Tag 'C9' may depend on the actual implementation. An unattended terminal may be able to act automatically when a request for PSAM Update is received.

References

Section 2-13.7 page 2-13-14, Primitive Data Objects for the APACS Header.

1-9.27 Transaction State Information

The PSAM offers a service to keep the merchant informed of the current state during the transaction.

The terminal defines by the data element Info Level (bit 2) whether the PSAM shall send Message Codes to the Merchant Application Handler (Merchant Interface).

References

PSAM State Information: Section 2-5.1.3 page 2-5-6, Restart.

Transaction State Information, command: Section 2-14.6.22 page 2-14-102.

1-9.28 Local PIN

The PSAM offers a functionality where a reference PIN is conveyed to the PSAM (in plaintext or enciphered) and compared internally with a PIN entered on the PIN Entry Device (PED) by the cardholder. The PSAM will return the result of the comparison.

Both plaintext or enciphered reference PIN can be used. It is recommended to use the enciphered reference PIN, as this solution enhance the security by offering confidentiality and reduce the possibility for performing replays. This is accomplished by adding a validation of a transaction counter given by the Local PIN application with the transaction counter maintained by the PSAM.

References

Section 2-12 page 2-12-1, Local PIN.

Commands: Section 2-14.8 page 2-14-122, Local PIN Commands.

Data Elements: Section 2-15.3 page 2-15-48, Data Elements specific for the Local PIN Application.

ASW1-ASW2: Section 2-14.10.2 page 2-14-184, ASW1-ASW2 Applicable for Local PIN.

1-9.29 Placement and Installation of terminal

Introduction

How the terminal is placed in relation to the surrounding environment may influence on the risk of having the PIN code disclosed.

Also the placement of the terminal in relation to the position of the cardholder may influence on the cardholders capability to cover the PIN entry with the body and hands.

The fundamental design of the terminal shall be based on the requirements concerning the mounting of the PIN Entry Device in the terminal.

A number of additional requirements are defined for the placement and installation of the terminal.

During the design of a terminal, these requirements shall be considered and the construction of the terminal shall make it possible to comply with the requirements when the terminal is installed.

1-9.29.1 Mounting of the PIN Entry Device in the terminal

The mounting of the PIN Entry Device in the terminal shall guarantee a high level of comfort when the cardholder is using the terminal.

The design shall also ensure that no sensitive transaction data can be disclosed, e.g. by Shoulder Surfing.

The PIN Entry Device shall be mounted with the key-tops pointing at the cardholder.

NOTE: When the terminal is placed as intended, the key-tops on the PIN Entry Device shall point in direction of the cardholders eyes.

The mounting of the PIN Entry Device should prevent successful installation of a Tapping Device on the top of the PIN Entry Device.

NOTE: The top of the PIN Entry Device visible from the outside of the terminal should prevent that a Tapping Device should be fixed or just 'clicked' to the top.

NOTE: To make sure that unauthorized access to the PIN Entry Device from the interior of the terminal will be detected, the screws or nuts by which the the PIN Entry Device is fixed may e.g. be sealed.

1-9.29.2 Placement of the terminal

When the terminal is setup in the environment where it is going to be used, the position of the terminal shall guarantee

a high level of comfort for the cardholder, including the possibility to get close to the terminal.

The position of the terminal in relationship with the cardholders working position shall also ensure that no transaction data can be disclosed, e.g. by Shoulder Surfing.

The requirements defined in this section may not be possible to comply when the terminal is designed, because the level of compliance may be a result of the installation and placement of the terminal at the Merchant. But during the design and development of a terminal these requirements shall be considered.

When the terminal is installed as intended the center of the surface on the '5'-key shall not be placed below 800 millimeter, measured from the floor-level where the cardholder is standing when using the terminal, see figure 2-7.5 page 2-7-12

When the terminal is installed as intended the center of the surface on the '5'-key shall not be placed above 1250 millimeter, measured from the floor-level where the cardholder is standing when using the terminal, see figure 2-7.5 page 2-7-12

It is recommended that the Attended terminal is placed with the PIN Entry Device in a height between 900 and 1000 millimeter.

When the Attended terminal is installed as intended the PIN Entry Device shall be in an angle between Horizontal and 45 degrees to Horizontal, see figure 2-7.4 page 2-7-11

When the Unattended terminal is installed as intended the PIN Entry Device shall be in an angle between Horizontal and Vertical, see figure 2-7.4 page 2-7-11

It is recommended that the relation between the height of the PIN Entry Device and the angle to Horizontal follows the guidelines:

<u>Height (mm)</u>	<u>Angle (degrees)</u>
800 - 900	0 - 30
900 - 1100	30 - 60
1100 - 1250	60 - 90

When the terminal is installed as intended the distance from the center of the surface on the '5'-key to the front of the terminal shall not exceed 200 millimeter, see figure 2-7.5 page 2-7-12

NOTE: The front of the terminal is defined as the vertical level of the terminal (or the base on which the terminal is placed), which restricts the cardholders possibility of getting close to the terminal.

The terminal shall be placed under consideration to mirrors, video cameras, staircases or other similar conditions in the environment.

NOTE: The terminal shall be placed like no view towards the PIN Entry Device is possible within the 'opening' angle not shielded by the privacy shield or the cardholder's body.

Reference

See chapter 2-7 page 2-7-1, Privacy Shield on PIN Entry Devices.

1-10 Functionalities

1-10.1 Introduction

This section contains the requirements for different functionalities in an OTRS terminal. It starts with a listing of the basic calls to the PSAM. This is followed with section on additional functionalities. They are;

- **Cash**
There are special requirements for manual cash disbursement when not using ATM's.
- **Terminal Services**
Special Terminal services may be required in certain regions and/or business environments.
- **Processing Condition Table**
The handling of a table that makes it possible to remotely configure some of the capabilities of the terminals.
- **Special status features**
The PSAM has the capability of returning a status of a previous transaction and to perform duplicate transaction check.
- **Prepaid ICCs**
This functionality enables the use of ICC based prepaid cards, normally issued in closed areas. The cards are not associated with a bank account.
- **Prepaid MSCs**
This functionality enables the use of MSC based prepaid cards issued by groups of stores etc. and not associated with a bank account.
- **Loyalty information**
This functionality enables the Merchant to retrieve loyalty information. This is possible for ICC as well as for MSC cards.
- **Token based transactions**
Token transactions are used when the exact amount is unknown when the payment sequence is initiated. The functionality is, for attended terminals, typically used in Hotels, Restaurants and Card Rental business. It is, for Unattended Payment Terminals, typically used for Automated Fuel Dispensers and ticket vending machines.
- **Special functions**
Function related to the use of Terminals in special environments.
- **Dynamic Currency Conversion (DCC)**
This functionality enables the cardholder to use his own currency different from the merchants currency. This functionality is so far only specified for attended terminals and not yet for Unattended Payment Terminals.
- **Tips/Gratuity**
This functionality supports the addition of an extra amount to the basic payment. This functionality is typically used in Hotels and Restaurants. Addition of Tips/Gratuity may be based on the use of tokens.

There is a subsection for each functionality. Special requirements may emerge when the above mentioned functional-

ities are combined. An example of this is an attended terminal in the hotel environment supporting tips.

Many of the requirements listed in this chapter are only mandatory for certain regions. Information on, whether or not this is the case, can be found in the different sections of Chapter 1-15 Regional requirements.

Requirements for receipts are covered in chapter 1-12 Receipts.

1-10.2 Business Calls to the PSAM

The sections that follows enhances the description of the different business calls given in section 1-9.4.

1-10.2.1 Purchase

Purchase is used when the transaction is completed as a single operation. Normally, the cardholder and card will be present during the entire transaction. The exact transaction amount must be present before the transaction can be completed.

Depending on the card type, the amount etc., the Purchase can be performed either offline or online and may result in either:

- an online Financial Request or
- generation of a Financial Advice

The Purchase may be seen as a complete transaction flow when goods or services are paid in a retail business environment or similar.

In some cases, a physical card may not be present when performing Purchase transactions. In these cases, the card number and other data is manually keyed in. This is normally only possible if allowed by the acquirer and card issuer.

1-10.2.2 Original Authorization

The Original Authorization transaction is used when the exact transaction amount is not known up front but authorization of the card and the estimated amount needs to be obtained before a service can be delivered. The Original Authorization will initiate the process for authorization, either online or offline, but no financial message will be generated.

Examples are hotels where the card and expected amount are authorized at check-in and the "real" transaction (called Capture) is performed at check-out when the exact amount is known. Similar examples are car rentals and self-operated petrol stations.

The output from an Authorization transaction (of either type) is called a Token.

A Token is a string of data created by the PSAM for later use as input to the Capture transaction. The Token includes the

information necessary to link the Original Authorization with the subsequent and resulting Capture.

The Capture transaction can be performed with a PSAM different from the PSAM creating the Token, e.g. if the check-in and check-out counters in a hotel have different terminals. In this case, the Token could be stored in a back office computer system and thereby be available to more terminals. Generally, the Token is stored in the Merchant Application.

The estimation of the amount may be dependent on the acquiring agreement and the card type.

- For MSC transactions the PAN/Prefix may be used to select the card type and with that estimate the amount.
- For EMV transactions the AID may be used to select the card type and with that estimate the amount.

1-10.2.3 Extended Authorization

The Extended Authorization transaction offers a way to identify a specific card without revealing card sensitive data such as PAN and PAN Sequence Number. Some cards may have the same PAN and only differ in the PAN Sequence Number but not all cards contains a PAN Sequence number. A revised version of the Business Call is thus introduced to take this into account. An Extended Authorization can thus be issued in two different ways;

- As the backward compatible version, using TR = 07 only based on the PAN. This will generate a *Submit Card Reference* command from the PSAM with a single card reference.
- As an updated version, using TR=09, taking information of the PAN sequence number into account. This will generate a *Submit Card Reference2* command from the PSAM with a Dual Card Reference.

Card Reference information (computed by use of a cryptographic algorithm) is given in the *Submit Card Reference(n)* command issued by the PSAM.

The *Submit Card Reference(n)* command is issued by the PSAM immediately after the last *Read Record* or *Internal Authenticate* command.

- | | | |
|------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.2.3.1 | B | A terminal implementing Extended Authorization shall only use a single method, i.e. either use TR=07 or use TR=09. The selection of method may be configurable. See 2-14.6.24 and 2-14.6.25 for further information.

For a terminal using the updated Extended Authorization returning Dual Card Reference, the following applies. |
| 1-10.2.3.2 | A | A card reference of '00 00 00 00 00 00 00 00' shall be interpreted as a non-existing card reference. |
| 1-10.2.3.3 | A | The terminal shall, if the reference is stored, store it together with the token. |
| 1-10.2.3.4 | A | The terminal shall, when searching for a card reference, if a primary value exists, start by using the primary value. |
| 1-10.2.3.5 | A | The terminal shall, if a match is not found in the first search, repeat the search using the secondary value. |

- 1-10.2.3.6 A The terminal shall, if a match on the secondary value is found on the repeated search, reject the search, if the primary value exists but does not match.

This unique Card Reference is particular useful for implementations like parking lots and gas stations, where it can be used to either identify the card at checkout (to compute the parking fee) or to identify the correct receipt.

Furthermore, the Extended Authorization transaction is also suitable for DCC transactions, as neither APE nor DAPE can be enabled and thereby interfere with the cardholder dialog.

The output from an Extended Authorization transaction is a Token (as for the Original Authorization).

For implementations which do not require the Token at the end but only the Card Reference, the transaction can be interrupted deliberately by the terminal. This is performed by returning a specific Response Code in the response to the *Submit Card Reference(n)* command.

Having obtained an unique Card Reference by interrupting the transaction, is not a guarantee that the succeeding payment transaction can be performed successfully. By completing the first transaction without interruption (and thereby creating a Token), the probability for a succeeding successful transaction will be close to 100%.

The Extended Authorization is limited to the following Card Data Sources:

- EMV
- MSC, including fallback

Example of use - Parking Scenario

Table 1-10.1 - Parking - Example - No PIN entry at Entrance

Parking lot (Purchase transaction)	
Entrance (No PIN)	Exit (PIN)
<ul style="list-style-type: none"> • The terminal performs an automatic Application Selection i.e. preferred or first application is selected. Cardholder is not involved. • An Extended Authorization transaction is initiated. The amount is limited and the authorization is used to verify that the card is valid. • (No CVM can be used). • During the transaction, a unique Card Reference is delivered to the terminal/System and saved along with time-stamp etc. for calculating the price of the parking. • The token is discarded. 	<ul style="list-style-type: none"> • The terminal performs an automatic Application Selection i.e. preferred or first application is selected, same procedure as used at the entrance. • The cardholder will be presented with the same application as selected at the entrance. • Cardholder accepts the application (if needed). • An Extended Authorization is initiated and a unique Card Reference is obtained. • The terminal interrupts the transaction after the <i>Payment</i> command by responding with a specific RC when the Card Reference is delivered. Note: The terminal shall continue all the way to the <i>Payment</i> command to ensure a graceful termination in the communication with the user card. • Using the Card Reference, the terminal/system obtains the previously saved entrance time and is able to compute the exact parking fee. • A PIN-based purchase transaction is initiated (using the same application as selected above), i.e. without cardholder performed Application Selection. • Alternatively, the terminal can complete the Extended Authorization transaction (PIN-based), and after the exact fee is computed, initiate a Capture containing the correct amount.

Table 1-10.2 - Parking - Example - PIN entry at Entrance

Parking lot (Token Transaction)	
Entrance (PIN)	Exit (No PIN)
<ul style="list-style-type: none"> The terminal performs Application Selection according to the EMV rules involving the cardholder. An PIN-based Extended Authorization transaction is initiated. The amount is typically corresponding to the fee required for a maximum parking period. During the transaction, a unique Card Reference is delivered to the terminal/system. A token is created. The Card Reference is typically used as a search key for the token. 	<ul style="list-style-type: none"> The terminal performs an Application Selection choosing the first application. An Extended Authorization is initiated. If the Card Reference does not match any of the previously obtained and stored values, the transaction is terminated and next application is selected and an Extended Authorization is initiated again until a match is met. Note: This procedure will impact the offline counters in the card as well as the processing time! When the match is met, the terminal/system obtains the previously saved entrance time and is able to compute the exact parking fee. A Capture transaction using the token and the computed parking fee as amount.

Example of use - Gas Station

Table 1-10.3 - Gas Station - Example - PIN before filling

Gas Station	
Before filling (PIN)	After filling – Receipt (No PIN)
<ul style="list-style-type: none"> The terminal performs Application Selection according to the EMV rules involving the cardholder. A PIN-based Extended Authorization transaction is initiated. The amount is typically corresponding to the value of a maximum capacity of the car. During the transaction, a unique Card Reference is delivered to the terminal/System. A token is created. When finishing the filling up, a Capture is initiated containing the full/correct amount. 	<ul style="list-style-type: none"> A: One mutual supported application: The cardholder inserts the card and an automatic Application Selection is performed. A: An Extended Authorization is initiated. If there is a match with a previously stored Card Reference and the corresponding Capture is completed, a receipt is automatically printed and the transaction terminated. If the Card Reference is not matching the cardholder card, he will be asked if he wants to fill up the tank and select the pump (see the previous column). B: Multiple mutual supported applications: The terminal performs an Application Selection choosing the first application. B: An Extended Authorization is initiated. If the Card Reference is not matching any of the previously obtained ones, the transaction is terminated and the next application is selected and an Extended Authorization is initiated again until a match is met. <i>Note that this procedure will impact the offline counters in the card!</i> When the match is met, a receipt is printed. If the Card Reference is not matching the cardholder card, he will be asked if he wants to fill up the tank and select the pump (see the previous column).

NOTE: The scenarios given above are merely examples. There might be other (and perhaps more suitable) ways to take advantage of the opportunities, that the Extended Authorization transaction provide.

1-10.2.4 Supplementary Authorization

If the transaction amount exceeds the previously authorized amount(s), e.g. when a hotel guest decides to stay longer, the Token from the previous Authorization transaction is used as input to a Supplementary Authorization transaction in order to increase the previously authorized amount(s). The Additional Authorization transaction can be performed with a PSAM different from the PSAM creating the Token.

One or more Supplementary Authorizations may follow an Original Authorization and the amount specified in an Supplementary Authorization shall be the difference between the new estimated amount and the amount already authorized.

The card is not involved for the Supplementary Authorization transaction as all necessary information is stored in the Token. Hence, the Token given as output from the Original Authorization (or from preceding Supplementary Authorization(s)) shall be used as input to the Supplementary Authorization. The Token includes the necessary information concerning the card data, and therefore the card is not required/used when an Supplementary Authorization is initiated.

The Supplementary Authorization will always initiate an online Authorization Request, but no financial message will be generated. The Token will be updated accordingly and given as output, i.e. the new Token will replace the old.

1-10.2.5 Capture

Capture is used when the exact amount is known (Accurate Amount) after the process of paying with a card was initiated using an Original Authorization (including any potential Supplementary Authorizations).

The Token from the last performed authorization shall be used as input, and since the authorization has already been approved, the generation of a Financial Advice will be performed offline. The physical card is not involved for this transaction type as all necessary information is stored in the Token.

A given Token must never be used for more than a single Capture transaction.

Examples:

When paying for goods from a fuel dispenser (or in other similar situations) an Original Authorization shall be completed successfully before the delivery of fuel is started and a Capture shall be initiated when the delivery is completed.

In a hotel environment (or in other similar situations) the Original Authorization call may be used at the time of check-in, while the Supplementary Authorization may be used to increment the amount authorized during the stay at the hotel. At the time of check-out a Capture shall be initiated

In a restaurant environment (or in other similar situations) where the adding of gratuity to the card transaction is possible, the Original Authorization call may be used when the cardholder asks for the bill, and the Capture call shall then be used to complete the process of paying with the card, when the cardholder has signed the bill and the value of gratuity is known.

1-10.2.6 Refund

If, for some reason, the cardholder and merchant agrees that funds shall be transferred from the merchant to the

cardholder, the Refund transaction is used. An example could be that the cardholder returns some goods. Even if the goods were paid for by the same debit/credit card, no previous transaction data is used for this transaction type.

The Refund call may be interpreted as a "Purchase with negative amount value" and will be used e.g. when the cardholder returns some goods for which a Purchase or Capture has been completed in another branch.

1-10.2.7 Authorization Reversal

If it is realized that the Token from a previous Authorization transaction will never be used or if the pre-authorized amount is much higher than the expected amount for a Capture transaction, a Reversal (Authorization) may be initiated. The purpose of this is to adjust the cardholder's spending limit in the issuer system.

The physical card is not involved for this transaction type as all necessary information is stored in the Token.

In case of technical errors, the PSAM may automatically generate Reversals for financial transactions (Purchase, Capture and Refund transactions). Such reversals cannot be initiated by the Merchant Application.

1-10.2.8 Cancellation

Introduction

The functionality of Cancellation is typically utilized in situations where the merchant has entered an incorrect amount and performed a successful purchase transaction before the merchant/cardholder has discovered the mistake, i.e. Cancellation is mainly applicable to attended terminals.

A cancellation may as well be automatically initiated in an UPT, if the terminal detects that it cannot deliver the goods purchased, e.g. when a ticket cannot be printed.

Whenever a successful purchase transaction is performed, the PSAM stores an image (copy) of the transaction internally.

Due to this image kept inside the PSAM, a new insertion/swiping of the card or key entering of card data is *not* required when initiating a Cancellation transaction.

Transaction flow

The Business Call Cancellation is divided into the same four steps/commands as the other transaction related Business Calls:

- Initiate Cancellation Payment,
- Cancellation Payment,
- Validate data and
- Complete Payment.

The format of the commands and responses can be found in section 2-14.7.

- 1-10.2.8.1 A The terminal shall, in certain regions support the Business Call Cancellation.

- 1-10.2.8.2 A The Cancellation Business Call shall never be cardholder initiated.
- 1-10.2.8.3 A The terminal shall only enable a Cancellation if the previous Business Call was a successful Purchase transaction.
- 1-10.2.8.4 A The terminal shall only enable a Cancellation for a “revoke” period of 10 minutes after the Purchase.
- The period in which it will be possible to perform a Cancellation is dependant upon an agreement between the terminal supplier and the merchant. See also section 2-5.15.2, “The Transfer of Advices” page 2-5-101.
- 1-10.2.8.5 A The time-out value for the period in which it will be possible to initiate a Cancellation shall be configurable.
- NOTE:** The time-out value can have a maximum value of 10 minutes
- 1-10.2.8.6 A The default value for the period in which it will be possible to initiate a Cancellation shall be 10 minutes.
- 1-10.2.8.7 C The terminal may either inhibit the use of Cancellation or generate an error message, if an attempt is made to use the Business Call when not applicable. The error message used shall be message code 'FF', “Invalid transaction”.
- 1-10.2.8.8 C The terminal may, if the previous Business Call was an Authorization, guide the merchant to use the Business Call Reversal of Authorization instead of the Cancellation.
- 1-10.2.8.9 B The terminal shall, prompt the merchant for a confirmation before completing the Cancellation transaction.
- 1-10.2.8.10 C The terminal may present information on the Amount and Date & time to the merchant to guide him/her in proceeding with the transaction.
- NOTE:** This information is provided by the PSAM in the response to the *Initiate Payment* command.
- 1-10.2.8.11 A The terminal shall not display any information about the PAN.
- 1-10.2.8.12 A The terminal shall allow the merchant to interrupt the Cancellation. It shall not be possible to resume an interrupted Cancellation.
- 1-10.2.8.13 A The terminal shall indicate this interruption by returning a Transaction Status of “Declined” in the *Complete Payment* command. See section 2-14.6.4 for details.
- 1-10.2.8.14 B The terminal shall, when interrupting the Cancellation skip the *Payment* and *Validate* commands.
- A Cancellation transaction is always performed offline. A successful Cancellation will delete any corresponding Financial Advice stored in the Data Store, and generate a Reversal Advice.
- 1-10.2.8.15 A The terminal shall support the following TAPA commands

- Get File Record
- Delete File Record

NOTE: These commands are issued by the PSAM during the Cancellation transaction. The Get File Record command is used to check if the previously created Financial Advice still is present and valid. The Delete File Record command is used to delete the previously created Financial Advice, when all the conditions for performing a Cancellation transaction is fulfilled.

1-10.2.8.16 A The terminal shall not initiate an Advice Transfer, an Advice Enclosing or an Advice Forwarding of the most recent Financial Advice within in the time frame for Cancellation.

NOTE: Transferring the most recent Financial Advice will disable the possibility of a Cancellation of that transaction.

1-10.2.8.17 A The terminal shall generate a Cancellation receipt when the transaction is successful. The receipt shall contain all of the content of the original receipt. The receipt shall as well contain a "Cancellation indicator" in line TR4.

NOTE: The PSAM will not (cannot) return information on Surcharge, Extra and DCC information. It is thus necessary for the terminal to keep an image of the previous receipt in order to be able to generate an Cancellation receipt.

NOTE: It is not necessary for the terminal to store any of the data previously transferred to to the host. The PSAM will take care of this, including any additional "envelope" data.

NOTE: It is possible to distinguish a Reversal Advices created as part of Cancellation transaction by the value of the Message Reason Code (MRC). The value of 4005 (Original amount incorrect) indicates that a Cancellation transaction has been performed.

1-10.2.8.18 A The terminal shall not generate any receipt, if the Cancellation transaction fails.

1-10.2.8.19 A The terminal shall not generate any entry in the Terminal Report, if the original Purchase transaction generated a Financial Advice, and this Financial Advice has not yet been included in the Terminal Report.

1-10.2.8.20 A The terminal shall generate a corresponding entry in the Total Report, if the original Purchase transaction was an online MSC transaction, or if the corresponding Financial Advice already has generated an entry in the Total Report.

1-10.2.8.21 C The information should be stored in a special 'cancellation' group, and not in the 'refund' group, as the handling of a Cancellation transaction will differ from the handling of a Refund transaction. A Refund transaction may include a surcharge to be paid by the cardholder in the total amount.

- 1-10.2.8.22 A The terminal shall handle a purchase transaction and a corresponding Cancellation as a voided transaction in the total report.

The flow for the different elements of a Cancellation transaction is shown in section 2-5.5 through 2-5.8.

1-10.3 Cash

Special requirements exist for non-ATM manual cash disbursement. These requirements are listed in this section.

- 1-10.3.1 A The terminal shall generate a receipt as specified in section 1-12. See an example of a Cash receipt in receipt "O" in section 1-12.4.15.
- 1-10.3.1.1 A The merchant's receipt shall, in extension to the normal information, provide fields for the following additional information;
- A recording of the the four first digits of the PAN printed on the front of the card (printed below the embossing).
 - The bearers name (if different from the name on the card).
 - Description of type of personal identification requested (like passport, drivers license etc.),
 - Unique identification number (like passport/driver's license number)
 - Jurisdiction of issue.
 - Expiry date of identification.
- 1-10.3.1.2 A The terminal shall either support the manual (key) entry of the above information, or provide fields on the receipt, where the information can be manually entered.
- 1-10.3.1.3 A The terminal shall **not** be able retrieve the information from the magstripe or the chip data.
- 1-10.3.1.4 A The terminal shall, if data is key entered, ensure, that the processing of the transaction cannot proceed before all of the above mentioned information has been entered.
- 1-10.3.1.5 A The Cardholders receipt shall, for some regions, contain a "Cash fee Info" field. See section 1-12.2.9 lines SI19 - SI22

1-10.4 Private Label Card Scheme Recognition

It may be desired to detect certain Private Label Card schemes, and enable the processing by the Terminal/Cash Register. The requirements for this function are listed in this section.

- 1-10.4.1 A A terminal shall, if it wants to evaluate if a card belongs to a valid private label card scheme, issue a *Get Debit/Credit Properties* command with an Identifier of '0012'.

The *Get Debit/Credit Properties* command will return the requested track(s) in clear text if the following conditions are fulfilled:

- Track2 recognized to be “non-ISO” coded
- Track2 recognized to be “ISO” coded and recognized in the PSAM MSC table to be a Private Label Card
- Track2 is not present at all (this requires that the transaction is not initiated if the Card reader detects a read error reading Track2)

The algorithm to decide if a Track2 is recognized to be “non-ISO” is as follows:

- PAN more than 19 digits
- PAN less than 8 digits
- More than 19 bytes

If Track2 has 2 or 3 separators it will be recognized as an “ISO” Track2 only if:

- If 2 separators, they must be placed after each other (==) or with 4 digits in between (=nnn=)
- If 3 separators, they must be placed after each other (===).

Discretionary data will *not* be included in the Track2 “ISO” check.

- 1-10.4.1.1 A The terminal shall only allow that the information is used for further Private Label Card scheme processing in the Terminal/Cash Register, if bit 8 =“1” in the Card Service Info field in the response to *Get Debit/Credit Properties* command.

- 1-10.4.1.2 C A Terminal may perform normal PSAM-based transactions using cards from a Private Label Card Schemes like any other card type, provided the BIN range is allowed in the tables supplied from the PSAM.

1-10.5 Terminal Services

This subsection specifies terminal services that may be implemented in certain regions/business environments.

1-10.5.1 Additional Card BIN Information

The PSAM is able to provide the terminal with additional information on the BIN range of the card used. This is for instance used by the DCC service.

- 1-10.5.1.1 A The terminal shall use an empty Amount field when issuing the *Initiate Payment 2* command to be able to receive the data.
- 1-10.5.1.2 C The terminal may retrieve information on the BIN range from the *Get Amount 3* command that will follow from the PSAM. This will include the masked value of the PAN, See section 2-14.6.29 for further details.

1-10.5.2 Additional Transaction Information

The PSAM has a capability for transferring additional merchant/acquirer/issuer specific data. This includes data transfer from as well as to the terminal from the Host.

A standard use of this capability is the DCC service and Swedish regional data. Besides of that, the use of this data transfer capability is customer specific and must be agreed for each use. The use requires that special handling of the data is implemented on the host. The functionality is implemented using the *Set Debit/Credit Properties* and *Get Debit/Credit Properties* commands. The commands are specified in details in section 2-14.5.8 and 2-14.5.9.

Two variants of the functionality exist, the Issuer Envelope and the Extended Issuer Envelope.

- 1-10.5.2.1 C The terminal may use the Issuer Envelope and the Extended Issuer Envelope at the same time.
- 1-10.5.2.2 C The Issuer Envelope Data and the Extended Issuer Envelope Data may contain multiple data sets, each identified by a 2-byte tag and the corresponding length field of 2 bytes. The data sets are specified for the individual functionalities.

NOTE: DCC and regional Swedish terminals are examples of standard data sets.

Terminal Settings

- 1-10.5.2.3 A When Extended Issuer Envelope is going to be utilized, the *Set Debit/Credit Properties* command (identifier = '8001') shall be sent prior to the *Exchange Debit/Credit Static Information* command, indicating in the Terminal Settings bit b8 that Extended Issuer Envelope is used.

NOTE: Supporting Extended Issuer Envelope may require an extended file size in *Get Debit/Credit File Characteristics* command response (up to 1024 bytes). The data element Terminal Settings can be found in section 2-15.2.150.

Buffer size

- 1-10.5.2.4 C The Terminal may request information about the space available for the Issuer Envelope and the Extended Issuer Envelope together using the *Get Debit/Credit Properties* command with an identifier of '0011'.

The command will return the maximum buffer sizes for the Issuer Envelope and the *total* buffer size for Issuer Envelope

and Extended Issuer Envelope. Terminals not using Issuer Envelope for e.g. DCC will therefore have more space in the Extended Issuer Envelope than a terminal also supporting DCC.

For Extended Issuer Envelope, if the data exceeds the total space available inside the PSAM, the transaction will be rejected. For Issuer Envelope, the transaction will be performed once data has been written to the buffer.

NOTE: The overall space available depends on space used by other elements as well.

- 1-10.5.2.5 A The terminal shall ensure that total of the data transferred to the two envelopes are within the space available.

Data conveyed from the Terminal to the Acquirer/Issuer

- 1-10.5.2.6 A If terminal data are going to be conveyed to the acquirer/issuer using the Issuer Envelope, the terminal shall perform a *Set Debit/Credit Properties* command with the Identifier = '8000'.

In case of several commands, the data given in a subsequent *Set Debit/Credit Properties* ('8000') command will overwrite the data given in the previous command.

- 1-10.5.2.7 A If terminal data are going to be conveyed to the acquirer/issuer using the Extended Issuer Envelope, the terminal shall perform a *Set Debit/Credit Properties* command with the Identifier = '8004'. The capability shall be activated in advance, see 1-10.5.2.3.

In case of several commands, the data given in a subsequent *Set Debit/Credit Properties* ('8004') command will be appended to any data previously written to the buffer.

In this way, it is possible for the terminal to add data for inclusion in the Authorization Request message, then clear the buffer and have nothing included in the Financial Advice later on. If the additional transaction data should be present here, obviously, the buffer should not be cleared. Finally, by using this mechanism, it is possible to include different data in the request and advice message.

NOTE: This deviates from the way the "old" Issuer Envelope behaves. It will overwrite any previous data.

- 1-10.5.2.8 A The terminal shall format data correctly, as no formatting of data will be added by the PSAM. The PSAM will not validate format information either.

- 1-10.5.2.9 C The terminal may 'clear' the envelope data by writing data to the envelope with a length of '00'. All previous stored data will be cleared.

- 1-10.5.2.10 A The terminal shall write the data to the envelope after the *Initiate Payment* command and before the *Payment* command if they are to be a part of an Authorization/Financial Request.

NOTE: Data written before the *Payment* command will as well be a part of any subsequent Advice, unless the buffer has been modified or cleared.

- 1-10.5.2.11 A The terminal shall write the data to the envelope before the *Complete Payment* command if they are to be part of a Financial Advice.

NOTE: Data written after the *Payment* command will only appear in the Financial Advice, if such a message is generated.

NOTE: The token generated by the PSAM in an Authorisation does **not** hold any information on the Envelope(s). The terminal must itself store and retrieve any Envelope information to be used in the Capture. This could be in the plaintext part of the token.

NOTE: Issuer Envelope Data that are sent during an Original authorization is **not** automatically sent again by the PSAM during the Capture. The terminal may attach these data to the token in order to convey them in the Financial Advice (Capture).

Data conveyed from the Issuer to the Terminal

- 1-10.5.2.12 A If acquirer/issuer data is going to be retrieved from the Extended Issuer Envelope, the terminal shall performed a *Get Debit/Credit Properties* commands with the identifier = '0010'.

NOTE: Currently, no mechanism is available to retrieve issuer data from the Issuer Envelope.

- 1-10.5.2.13 A It is the responsibility of the terminal to interpret the tags received with respect to the card type used for the transaction. Tags may overlap.

- 1-10.5.2.14 A The terminal shall read the data from the Extended Issuer Envelope after the *Validate* command and before the *Complete* command.

Specific Applications

This section holds the specification of the specific use of the Extended Issuer Envelope. See section 2-13.9.15 for more information.

- 1-10.5.2.15 B A terminal shall implement the handling of the "Customer Reference Number" additional data field. The data are to be sent from the Terminal to the Host. The tag to use is "4N". The field is of the type "an" with a maximum size of 32 characters.

NOTE: This information is normally provided by the POS. The Terminal will only transfer it to the PSAM.

NOTE: The data transferred to the acquirer and issuer may be limited to the first 20 characters during processing.

- 1-10.5.2.16 B A terminal shall, for special applications, implement the handling of the following additional data fields.
- "Receipt Number", tag "40" from the Terminal to the Host. Type ans10.

- "IFSF Field 48", tag "4P" from the Terminal to the Host.
- "IFSF Field 62", tag "4Q" from the Host to the Terminal.
- "IFSF Field 63", tag "4R" from the Terminal to the Host.
- "VAT percentage and Product type", tag "4T" from the Terminal to the Host.
- "Entry - Exit station", tag "4W" from the Terminal to the Host.
- "Supplier and Service Point info", tag "4Z" from the Terminal to the Host.

NOTE: This information is generated by/shall be provided to the POS.

1-10.5.3 Account Type Selection

This section specifies the requirements for Account Type Selection. This is a required service for some card types in certain regions.

- | | | |
|-------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.5.3.1 | B | The terminal shall, for ICC's, support Account Type Selection, when the ICC requests data element with tag '5F57' in the PDOL. |
| 1-10.5.3.2 | B | The terminal shall, for MSC's, support Account Type Selection, if the terminal has a PCT, the PCT has a ATS data element and PCT is enabled. |
| 1-10.5.3.3 | C | The terminal <u>may</u> shall not try to support Account Type Selection for ICC's based on the use of a PCT and BIN range from the customer part of the terminal. |
| 1-10.5.3.4 | B | Account Type Selection (debit or credit) shall be possible on the customer part of the terminal/when the terminal is operated by the cardholder. |
| 1-10.5.3.5 | B | The terminal may support, that merchant can perform the Account Type Selection. |
| 1-10.5.3.6 | A | The cardholder shall be able to select between "Debit" (code = 20) and "Credit " (code = 30). See section 2-15.2.1. |
| 1-10.5.3.7 | A | The enabling/disabling of Account Type Selection for MSC's shall be based on the PCT information, see section 1-10.6.4. |
| 1-10.5.3.8 | A | The cardholder's choice of account type shall be printed on the receipt, see requirement 1-12.2.9.11 page 1-12-16. |
| 1-10.5.3.9 | A | The cardholder's choice of account type shall be included in the <i>Initiate MSC/ICC/Key Entered Payment</i> command. |
| | | NOTE: The information is transferred to field 3 (Processing code) position 3 and 4 of the APACS messages. See section 2-13.9.2. |
| 1-10.5.3.10 | A | The terminal shall, for certain regions, when data are non-zero, as well store the information about the account type selected in the Issuer Information Envelope data, using tag "Z6". |
| 1-10.5.3.11 | A | The terminal shall, in a token based payment, store the Account Type information in the business specific part of the token. It shall retrieve the information at the Capture and return it in the <i>Initiate Token Based Payment 2</i> command. |

1-10.5.4 Cashback

This section specifies the requirements for the use of explicit cashback. This is a required service for some card types in certain regions.

- 1-10.5.4.1 A Entry of cashback shall either be activated as a special entry mode or as an additional step during Purchase.
- 1-10.5.4.2 A The enabling/disabling of the cashback shall, if a PCT is used, be based on the PCT information, see section 1-10.6.4.
- 1-10.5.4.3 C A terminal may, if a PCT is not used, have a manual way of enabling and disabling cashback.
- 1-10.5.4.4 A Entry of cashback amount shall be possible on the merchant part of the terminal.
- 1-10.5.4.5 C Entry of cashback amount may be possible on the cardholders part of the terminal.
- 1-10.5.4.6 C Indirect entry of cashback, as entry of the total amount, may be implemented.
- 1-10.5.4.7 A If the cardholder gets back cash in connection with a purchase, the cashback amount shall be included either in the *Initiate Payment* command in the "Amount, Other" field or as "Amount, Other" in the response to the *Get Amount 3* command from the PSAM.
- 1-10.5.4.8 A The receipt shall contain the cash back amount, see requirement 1-12.2.8.15.

The choice of cashback is included in field 3 (Processing code) position 1 and 2 of the APACS messages. See section 2-13.9.2. The cashback amount is included in field 8 (Amount Other) of the APACS message.
- 1-10.5.4.9 A Cashback shall not be enabled for DCC transactions.

NOTE: This is a Card Scheme requirements.

1-10.5.5 VAT

This section specifies the handling of VAT. Entry and reporting of VAT information may be required in some regions.

The VAT amount may be calculated using a default VAT percentage set in the terminal parameter table (currently 25%).

- 1-10.5.5.1 B The terminal shall be able to calculate and print a VAT amount.
- 1-10.5.5.2 B If the terminal is capable of printing the VAT amount, a merchant function for changing the VAT amount shall be available. The changed amount shall be checked for not being greater than calculated using the default VAT percentage.

NOTE: This function is used when the VAT amount for some reason is less than the automatically calculated VAT amount.

NOTE: An ECR or merchant unit may contain functions for VAT calculation using VAT percentages relevant for

the merchant. This may include functions for setting the normally used VAT percentages in the merchant unit.

NOTE: The VAT amount is calculated using the purchase/refund amount, only, i.e. any extra amounts are not included in the calculation.

- 1-10.5.5.3 A The total VAT Amount shall be included in the additional transaction data as shown in table 1-15.8.

1-10.5.6 Payment Condition Code

This section specifies the handling of Payment Condition Code. A Payment Condition Code is information about the conditions of the current transaction. The information is forwarded to the card issuer. Entry and reporting of Payment Condition Code information may be required in certain regions.

- 1-10.5.6.1 A If the terminal supports Payment Condition Code, then the merchant shall be able to enter a Payment Condition Code.
- 1-10.5.6.2 A The entry shall, for a SUT, be activated while the terminal is operated by the merchant.
- 1-10.5.6.3 C It may be possible to enable and disable the functionality in the terminal.
- 1-10.5.6.4 A If the merchant selects a Payment Condition Code for the transaction, the resulting data element Payment Condition Code shall be included in the additional transaction data as shown in table 1-15.8 and printed on the receipt as shown in requirement 1-12.2.9.7.
- 1-10.5.6.5 A The terminal shall, in a token based payment, store the Payment Condition Code information in the business specific part of the token.
- 1-10.5.6.6 A The terminal shall retrieve the information at the Capture and return it in the Issuer Envelope Data using the *Set Debit/Credit Properties* command.

1-10.5.7 Post Registration

Post Registration is a way to make either a purchase or refund when the cardholder is not present anymore.

Post Registration is intended to be used if either unexpected expends arises (e.g. parking tickets) or to pay money back if expends was lesser than expected.

Post Registration requires that the original payment was made as a token based transaction. It also requires that the token is kept after the original capture. The reason for this is that the token is now used as a "container" for a secure way to keep the PAN, Expiry Date and in some cases the CV-2 value.

Post Registration is applicable for EMV tokens, MSC tokens and Key Entered tokens. Post registration is **not** applicable for Track3 based tokens.

Seen from the terminal the transaction flow is like for a Capture with the exception that an online request may be expected. The host will receive the transactions as Key Entered transactions regardless of which of the token formats was used as input for the post registrations.

For a PSAM based terminal, the conversion from a Capture to a Key Entered transaction is made by the PSAM and is "hidden" for the terminal.

Two Business calls are defined:

- Post Purchase and
- Post Refund.

Post Purchase and Post Refund can be enabled/disabled individually by the PSAM Administrative System.

- | | | |
|------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.5.7.1 | A | The terminal shall process a Post Registration as a Key Entered transaction. |
| 1-10.5.7.2 | A | When Post registration is supported, the Token shall be kept after the Capture has been performed. When the business with customer is finished (and no more Post Registrations are expected), the Token shall be deleted. |
| 1-10.5.7.3 | A | It shall be assured that the a token used for a Capture can not be used to perform subsequent Captures. |

1-10.5.8 Acquirer Information

There is a requirement for additional information to the cardholder, when the merchant is able to select between different Acquirers. This information may be provided from multiple sources. The full information is named "Acquirer information". It consists of two data elements, an "Acquirer ID" and "Acquirer merchant number". The information will be available for online transactions. A complementary information to this is the "Acquirer Name" provided in the PCT, see section 1-10.6.4.

- | | | |
|------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.5.8.1 | B | The terminal shall, for certain regions, support "Acquirer Information". The terminal shall retrieve the information by Issuing a <i>Get D/C properties command</i> after Validate Data command, see section 2-14.5.8. |
| 1-10.5.8.2 | B | The terminal shall, if the information is available, print it in line TR7 of the receipt, see 1-12.2.9.19. |
| 1-10.5.8.3 | C | The terminal may print the information over two lines, if the data retrieved exceeds the line length. |
| 1-10.5.8.4 | A | The terminal shall, in a token based payment, store the "Acquirer Information" from the Authorization in the business specific information part of the token, to be available during the Capture. See figure 1-10.10 |
| 1-10.5.8.5 | B | The terminal shall, if no "Acquirer Information" is available, and the terminal supports "Acquirer Name" in a PCT, use the "Acquirer name" instead. |

NOTE: "Acquirer Information" takes priority over "Acquirer Name".

- 1-10.5.8.6 B The terminal shall, if neither “Acquirer Information” nor “Acquirer Name” is available omit line TR7 on the receipt.

1-10.5.9 Selectable Kernel Configurations

The PSAM will select the CVM to be used based on the Merchant Initiative and the following data elements;

- Terminal Capabilities,
- CVM configuration loaded in the PSAM,
- CVM list from the card.

It may, under specific conditions, be useful to change this selection.

An alternative configuration of the terminal may be selected. This could be a terminal without PIN pad while the basic configuration indicates that the PIN Pad is present.

The transaction can then be initiated using this alternative configuration. If this attempt is approved, then the transaction is completed in the normal way. If this attempt is rejected or fails, then the terminal may initiate a second attempt, using the basic configuration. If the second attempt is successful, the transaction can be completed in the normal way. If the second attempt fails, the transaction is completed unsuccessfully and the payment must be performed by other means.

The processing is from the cardholders point of view a single transaction. This requires a special set of display texts and special conditions for the number of receipts to be printed.

An alternative handling of the transaction can be achieved by use of the Selectable Kernel Configurations. The configuration is transferred from the terminal to the PSAM during the Initialization Sequence for the PSAM, see Figure 2-5.1. The alternative configuration is selected after this. Selection of configuration is performed for each transaction.

- 1-10.5.9.1 A The terminal shall, if the Selectable Kernel Configurations is supported, load the data into the PSAM using the *Set Debit/Credit Properties* command with an identifier of '8003'. See section 2-14.5.9 for further details.
- 1-10.5.9.2 A The Selectable Kernel Configurations shall be reloaded every time the PSAM has performed an Initialization Sequence.
- 1-10.5.9.3 A The command shall not be issued during the start up of the PSAM or while the PSAM is processing a transaction.
- 1-10.5.9.4 A The terminal shall set the Merchant Initiative to B'1xxx xx00 if it wants to select the Selectable Kernel Configurations. See section 2-15.2.93.

NOTE: The PSAM will return an ASW1-ASW2 = '1321' if the use of the Selectable Kernel Configurations is selected in the Merchant Initiative, MI, but is not loaded.

NOTE: Selectable Kernel Configurations can not be combined with Forced Signature or Forced PIN conditions.

NOTE: An empty command, i.e. Length_{INFO} = 0, will select of the basic configuration, see section 2-14.5.9 for further details.

- 1-10.5.9.5 A The Selectable Kernel Configurations shall only be selected for the following business calls;
- Purchase
 - Original Authorization
 - Extended Authorization
 - Capture
- NOTE:** A flow with signature during Authorization and NoCVM during Capture will be rejected
- 1-10.5.9.6 A The terminal shall, if an alternate kernel configuration is selected, update the POS entry mode in the *Initiate xxx Payment* command to reflect the change. See example in Table 1-10.4.
- 1-10.5.9.7 A The terminal shall, if a transaction is declined with the Selectable Kernel Configurations selected, not display the text message. '0C' "Not Accepted" or '07' "Declined". It shall instead display the message '0E' "Please Wait" on the Cardholder display while the second attempt is initiated selecting the basic terminal capability.
- 1-10.5.9.8 B The terminal shall, if a transaction is declined with the Selectable Kernel Configurations supported, but approved with basic kernel configuration capability, only generate a single approved receipt to the cardholder.
- 1-10.5.9.9 B The terminal shall, if a transaction is declined with alternative as well as basic kernel capability generate two declined receipts to the cardholder.

Table 1-10.4 - Selectable Kernel Configurations - Example

Data elements	Unattended	
	Alternative (No CVM only)	Basic (Online PIN only)
Terminal Capabilities	60 08 C8	60 40 C8
Additional Terminal Capabilities	60 00 B0 50 01	60 00 B0 50 01
Terminal Type	25	24
POS Capability Code	50X340	51X34C
POS Entry Mode	80X00X	20X00X

1-10.5.10 Preferred Offline processing

The preferred offline processing indicates, that it is preferred that the transaction is performed offline, but online processing is accepted, if required. The change in the transaction from offline to online is handled by the PSAM on-the-fly.

- 1-10.5.10.1 A The terminal shall set the Merchant Initiative to B'x111 xxxx if it wants to perform a Preferred Offline transaction. See section 2-15.2.93.

NOTE: There is no need/purpose of a second attempt if the Preferred Offline transaction fails.

1-10.5.11 Forced processing

The conditions for using forced processing are listed below.

- | | | |
|-------------|---|-----------------------------------------------------------------------------------------------------|
| 1-10.5.11.1 | A | The terminal shall, if it wants to force a PIN transaction, set the MI to B' 1xxx xx01. |
| 1-10.5.11.2 | A | The terminal shall, if it wants to force a Signature transaction, set the MI to B' 1xxx xx10. |
| 1-10.5.11.3 | A | The combined condition force PIN and force Signature shall not be generated. |
| 1-10.5.11.4 | A | The terminal shall, if it wants to force a the transaction on-line, set the MI to B'x101 xxxx. |
| 1-10.5.11.5 | A | The terminal shall, if it wants to force a the transaction of-line, set the MI to B'x110 xxxx. |
| 1-10.5.11.6 | A | A transaction using a forced condition, shall be declined, if the forced condition is not accepted. |

NOTE: The CVM list in some cards will decline the use of forced conditions.

1-10.5.12 Electronic Receipt Handling

Electronic Receipts makes it possible for the individual cardholder to receive receipt information as electronic information instead of as a piece of paper. The Electronic Receipt contains the information from the receipt and a unique reference to the card. The cardholder is then able to retrieve this information from an Electronic Receipt service provider. The service provider is named an Electronic Receipt Company or ERCo. Every ERCo will be identified by his own scheme ID. The Cardholder decides what ERCo's to sign up with.

The PSAM supports the use of Electronic Receipts. The PSAM is able to generate a unique reference for each PAN, a hash. The reference is generated using a one-way function. The reference is unique for each ERCo. The reference is based on the PAN and an ERCo unique salt.

The merchant may as well sign up with one or more ERCo's. The terminal may, for each transaction, generate one or more set of Electronic Receipts. Each Electronic Receipts consists of the receipt-information concatenated with the ERCo specific hash (reference). The receipts are sent to the different ERCo's.

Up to 32 different ERCo's can be defined, but the PSAM and the Host only supports up to 16 concurrent ERCo's.

The terminal may for each transaction, request a hash for one or more ERCo's based on the ERCo scheme ID's. The PSAM will return the hash for the ERCo's that are requested and identified.

- | | | |
|-------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.5.12.1 | A | The Terminal may request one or more references (hash values). The Terminal shall do this by issuing a <i>Get Debit / Credit Properties</i> command with an identifier of '0019'. See table 2-14.36 for further details. The return values will be formatted as shown in table 2-14.39. |
|-------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 1-10.5.12.2 A The terminal shall itself generate the Electronic Receipt(s) and send it to the individual ERCo's.
- 1-10.5.12.3 A The terminal may issue the request after the response to *Initiate XXX Payment* command has been received and before *Complete Payment* is issued.
- 1-10.5.12.4 C A Terminal may as well, for non contactless transactions, issue the request from receiving the *Get Amount* command and before the *Complete Payment* command is issued.

NOTE: It is, for contactless terminals, technically not possible to issue the request before the amount is known as the amount must be known before the card is read.

1-10.6 Processing Condition Table

1-10.6.1 Introduction

The Processing Condition Table, PCT, has been introduced to be able to convey specific parameters to a terminal. The data are forwarded using the PSAM as the transport provider.

The task of the PSAM is to convey the Processing Condition Table in a secure way like other updates sent to the PSAM. The PSAM will as well ensure that all entries in the table are coherent with respect to version. The PSAM does not enforce the processing conditions.

The terminal can get the content of the Processing Condition Table by issuing the *Get Processing Condition Table* command (along with the existing *Get Supported AIDs*, *Get D/C Properties* and *Get MSC Table* commands). The exact format of the *Get Processing Condition Table* command is described in section 2-14.5.12.

The availability of new Processing Condition Table information is flagged by the PSAM in the response to the *Start-up PSAM/Exchange Debit/Credit Static information* commands. The PSAM returns the ASW1-ASW2 = '1003' (New data available) in the response whenever the Processing Condition Table has been updated.

The requirements in section 1-10.6 are only applicable to terminals in regions where the use of a Processing Condition Table is required.

1-10.6.2 Data handling

The Processing Condition Table consists of a header and a body. The header contains version information and a Data Object List (DOL). The DOL is TLV encoded and specifies the data are stored in the records in the body of the table. The order of the data elements in the header is specified in the response to the command, section 2-14.5.12.

The decoding of the data and the order of the data in the body is given in the DOL in the header.

Each record in the PCT specifies the processing condition for a PAN prefix range. The PCT may contain multiple entries for a specific PAN prefix range. The more narrow prefix ranges are always real sub-ranges of the wider prefix ranges. The PCT will be delivered sorted, i.e. with the most narrow PAN prefix range first. The PSAM will deliver a complete PCT to the terminal.

- | | | |
|------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.6.2.1 | A | <p>The terminal shall, for a given PAN, select the most narrow prefix range from the PCT.</p> <p>NOTE: This can be achieved by using the first matching entry in the table, as the PCT will be delivered sorted.</p> |
| 1-10.6.2.2 | A | <p>The terminal shall be able to decode PCT data encoded in TLV format. The terminal shall decode the data in the body based on the Data Object List in the header.</p> <p>NOTE: Terminals are already required to handle TLV encoded data in the response to the <i>Select</i> command.</p> |

- 1-10.6.2.3 A The terminal shall be able to process a PCT header of at least 128 bytes and holding up to 32 data elements. The terminal shall be able to store a PCT body of at least 512 records, each of up to 48 bytes.
- 1-10.6.2.4 A The terminal shall neither update nor delete the existing Processing Condition Table before all of the updates to a new table has been retrieved successfully.
- NOTE:** The existing table is to continue to be operational, if the update of the table fails.
- NOTE:** The actual updates sent to the PSAM may consist of only a subset of the records in the PCT, but the terminal will always receive a complete table.
- There will be one list of applicable generic data elements and additional lists for each region including any of additional applicable data elements. These lists are found in section 1-10.6.5.
- 1-10.6.2.5 A The terminal shall decode any correctly TLV encoded data but discard elements not on the specified list(s) in this specification.
- NOTE:** As the PCT format is extended in the future, e.g. new data elements are added, the terminal software has to be amended accordingly, if the terminal is to take advantage of these new data elements. Old terminals may still use the old data elements without problems due to the use of the TLV format.

1-10.6.3 Processing

The following requirements are only applicable for terminals in regions where the use of a Processing Condition Table is supported.

If the terminal does not issue a "Get Processing Condition Table" command during Start-up, the PSAM will not require this command in succeeding Start-ups (where the PSAM indicates "New data available") i.e. old terminals or terminals outside regions supporting PCT can use a PSAM supporting PCT. This is applicable until the next time an Installation is performed, where the "history" will be reset.

Initialization

- 1-10.6.3.1 A When ASW1-ASW2 = '1003' (New data available) is returned in the response to either the *Start-up PSAM* or *Exchange Debit/Credit Static Information* command, the terminal shall issue the following commands:
- Get Supported AIDs
 - Get Debit/Credit Properties
 - Get MSC Table
 - Get Processing Condition Table
- See figure 2-5.1 for further details.
- 1-10.6.3.2 A When ASW1-ASW2 = '1000' (Configuration required) is returned in the response to either the *Start-up PSAM* or *Exchange Debit/Credit Static Information* command, the terminal shall issue the following commands:

- Get Supported AIDs
- Get Debit/Credit Properties
- Get MSC Table
- Get Processing Condition Table
- Get Debit/Credit File Characteristics
- Configure PSAM Application

See figure 2-5.1 for further details.

- 1-10.6.3.3 A The terminal shall start the *Get Processing Condition Table* command by requesting the header of the table.

NOTE: The information in the header is used to interpret the contents of the body.

- 1-10.6.3.4 A The terminal shall continue with the *Get Processing Condition Table* command, by requesting the body of the table, until all records has been read.

- 1-10.6.3.5 A The terminal shall stop the Get Processing Conditions Table sequence, if the ASW-ASW2 returned is '1021'(PCT not consistent).

NOTE: This may be the case if the update of the PCT is in progress inside the PSAM.

Transactions

It is the task of the terminal to enforce the processing conditions matching a given PAN prefix.

NOTE: The handling of the actual processing conditions is specified as regional requirements.

- 1-10.6.3.6 A When the PAN is available from the PSAM, the terminal shall check whether the processing conditions from the PCT have any impact on the current transaction.

- 1-10.6.3.7 A If the processing conditions indicates that the transaction in progress is not allowed, the terminal shall send a *Complete Payment* command immediately after the response to *Initiate Payment* command has been returned from the PSAM.

- 1-10.6.3.8 A If the processing conditions indicates that a specific capability shall be enabled/disabled, the transaction in progress shall be configured accordingly.

- 1-10.6.3.9 A The *Get Amount 3* command shall be supported by the terminal.

- 1-10.6.3.10 C The terminal should utilize "Late Amount Entry" when supporting the Processing Condition Table.

NOTE: By using "Late Amount Entry" the terminal has the opportunity to interrupt/decline the transaction when the *Get Amount 3* command is sent to the terminal.

This will prevent the cardholder from being engaged in the CVM handling (e.g. PIN entry) before declining the transaction.

NOTE: "Late Amount Entry" means that the *Initiate Payment* command does not contain any amount(s).

1-10.6.4 Processing conditions controlled by the PCT

This subsection specifies the way a terminal shall interpret the different processing conditions. As the processing condition is determined by the PAN, the processing conditions will only be known once the PAN is available.

Whether or not the functionality shall be enabled is defined in the regional requirements.

- 1-10.6.4.1 C The processing conditions specified below may be configurable in terminals without a PCT.

Cashback

- 1-10.6.4.2 A A terminal shall, if the processing condition "Cashback" is enabled not limit the use of cashback in the transaction due to processing conditions.

- 1-10.6.4.3 A A terminal shall, if the processing condition "Cashback" is not enabled, decline the transaction if it was attempted to use cashback.

- 1-10.6.4.4 A A terminal shall by default, i.e. if the PAN is not in any of the BINs specified in the PCT, **not** enable cashback. The terminal shall generate a receipt, if the cardholder has entered a PIN.

NOTE: Conditions, outside the PCT may limit the use of cashback anyway. This could be conditions in the terminal, the PSAM or conditions on the Host.

Key Enter

- 1-10.6.4.5 A A terminal shall, if the processing condition "Key Enter" is enabled, not limit the processing of key entered transactions.

- 1-10.6.4.6 B A terminal shall, if the processing condition "Key Enter" is not enabled, decline the transaction if it is a key entered transaction. The terminal shall not generate a receipt.

- 1-10.6.4.7 A A terminal shall by default, i.e. if the PAN is not in any of the the BINs specified in the PCT, **not** enable key entered transactions.

NOTE: Other conditions, outside the PCT may limit the use of key entered transactions anyway. This could be conditions in the PSAM or conditions on the Host.

Account Type Selection

- 1-10.6.4.8 A A terminal shall, if the processing condition "Account Type Selection" is enabled, activate the possibility for cardholder to select account type as specified in 1-10.5.3, show the selection on the receipt to be printed and record the information in the data sent to the host.

- 1-10.6.4.9 A A terminal shall, if the processing condition "Account Type Selection" is not enabled, not activate selection of account type, not print any information about it on the receipt, and not send any additional data on this to the host.

- 1-10.6.4.10 A A terminal shall by default, i.e. if the PAN is not in the BINs specified in the PCT, **not** activate selection of account type for the transaction.

NOTE: Account Type Selection, for ICC's, based on tag '5F57' in the PDOL shall not be affected by this.

- 1-10.6.4.11 B The cardholder shall, if the processing condition "Account Type Selection" is enabled, be able to perform "Account Type Selection" on the terminal.

- 1-10.6.4.12 C The merchant may, if the processing condition "Account Type Selection" is enabled, be able to perform "Account Type Selection" on the terminal.

NOTE: Other conditions, outside the PCT, like the transaction type, may limit the use of "Account Type Selection".

Acquirer Name

The "Acquirer Name" shall be printed on the receipt in certain regions. See chapter 1-15 for further information. The information shall be printed on line TR7 of the receipt, see section 1-12.2.9 for more information.

- 1-10.6.4.13 A A terminal shall, if the data object "Acquirer Name" is present, make it available for receipt generation.

- 1-10.6.4.14 A A terminal shall, if the data object "Acquirer Name" is requested, but **not** in the PCT replace it with a default value of all space characters (as the data element has a fixed length)".

- 1-10.6.4.15 A A terminal shall by default, i.e. if the PAN is **not** in the BINs specified in the PCT, replace the "Acquirer Name" with a default value of all space characters.

Bank at partner

Handling of the conditions "BIB" and "BIB Amount" is still under evaluation.

NOTE: "BIB" is a Swedish acronym for "Bank i Butik"

- 1-10.6.4.16 A A terminal shall, at the present, **not** react to the data elements "BIB" and "BIB amount".

1-10.6.5 Data Objects

Generic Requirements

Certain data providing configuration information, is mandatory to all Processing Condition Tables. The data objects listed in table 1-10.5 and 1-10.6 will be present in the response to the *Get Processing Condition Table* command for any region.

- 1-10.6.5.1 A A terminal implementing a PCT shall, when receiving a header, be able to decode any correctly TLV coded element.

Table 1-10.5 - List of Primitive Data Objects for use in the response to the *Get Processing Condition Table, get header* Command

Primitive Data Objects			
Tag	Attrib.	Length	Comment
'9F1A'	n3	2	Terminal Country Code
'DF60'	b2	2	VERSION _{PCT} . Version of the PCT
'DF61'	b1	1	SUBVERSION _{PCT} . Subversion of the PCT
'DF62'	n6	3	DATE _{PCT} . Date of creation (YYMMDD)
'DF63'	b1	1	Length of each record
'DF64'	b2	2	Total no. of records
'DF65'	n12	6	PCT PAN _{FROM}
'DF66'	n12	6	PCT PAN _{TO}
'DF6C'	-	var.	Data Object list (DOL)

NOTE: This is a list of possible objects. The order of the data objects in the header is specified in the command, see table 2-14.50.

Table 1-10.6 - List of Constructed Data Objects for use in the response to the *Get Processing Condition Table, get body* Command

Constructed Data Objects			
Tag	Attrib.	Length	Comment
'E3'	-	var.	Header

NOTE: The order of the data in the body is specified in the DOL in the header.

- 1-10.6.5.2 A Any terminal implementing a PCT shall be able to decode and use all of the data object in table 1-10.5.
- 1-10.6.5.3 A Any terminal implementing a PCT shall, once the DOL is available, be able to decode all of the data objects in table 1-10.6.
- 1-10.6.5.4 A Any terminal implementing a PCT shall, for maintenance and diagnostics purpose, be able to present the;
- Terminal Country Code,
 - Version,
 - Subversion,
 - Date and
 - No. of Records from the PCT.

Regional requirements

Further information on regional specific data element are found in section 1-15.

1-10.7 Special Status Services

Introduction

The PSAM offers two special services. The one is a check for duplicate transactions, the other is to provide the status of a previously performed transaction having financial impact.

These services are described in this section.

1-10.7.1 Duplicate Transaction Check by the PSAM

The PSAM includes a service for automatic control of identical/duplicate transactions.

How this check is performed is described in section 1-9.17 "Transaction Checks".

The number of minutes in which the duplicate transaction check is active may be modified utilizing the *Set Debit/Credit Properties* command, using Identifier '8002'.

The check may as well be disabled utilizing the same command.

The *Set Debit/Credit Properties* command is defined in section 2-14.5.9.

1-10.7.2 Status of Previous Transaction

Data being logged

Just before the PSAM returns the response to the *Complete Payment* command, the PSAM saves the following information concerning the current transaction if the ASW1-ASW2 indicates approved/successful:

- Reference STAN
- Amount
- Currency
- Currency Exponent
- Date/Time
- PAN

Search Keys

Two search keys exist in order to find transaction data for a particular transaction:

- Reference STAN
- PAN

NOTE: Both Reference STAN and PAN are returned in the response to the *Initiate Payment* command.

Data to be retrieved

The status of a previous successful transaction is obtained by issuing a *Get Debit/Credit Properties* command as described in the next section.

The PSAM will return the following information:

- Reference STAN
- Amount
- Currency
- Currency Exponent
- Date/Time

NOTE: The response from the PSAM does *not* include the PAN.

1-10.7.3 The Get Debit/Credit Properties Command

The *Get Debit/Credit Properties* command is among other things utilized to retrieve transaction status of previously performed transactions. The value of the "Identifier", which is part of the input parameters for this command, determines the search key:

- Identifier = '04' defines the search key is the Reference STAN
- Identifier = '05' defines the search key is the PAN.

Note that exact match of the PAN is a prerequisite for returning transaction data when using the "Identifier" equal to '05'.

When a match is found, the following data elements are returned:

- Reference STAN
- Amount
- CURRC
- CURRE
- DTHR

The format of the *Get Debit/Credit Properties* command/response is given in section 2-14.5.8 on page 2-14-29.

NOTE: Please note the limitations in usage given in section 1-10.7.5, "Limitations".

1-10.7.4 Purpose of this Functionality

Introduction

The status of previous transactions may be used in situations where the cash register system is inconclusive whether the current transaction is approved/successful or declined.

Each search key (Reference STAN or PAN) may facilitate different interfaces as well as different Transactions Requests (Purchase, Refund or Capture).

It is not recommended to use this feature every time a transaction is performed, as it will prolong the transaction time.

Reference STAN

When performing either a Purchase, Refund or Capture transaction, the STAN (=Reference STAN) is returned in the response to the *Initiate Payment* command.

If this Reference STAN is conveyed from the terminal to the cash register system at this point, the cash register system

have the opportunity to issue a *Get Debit/Credit Properties* command immediately after the final communication with the terminal if the *final* result of the transaction is inconclusive. See figure 1-10.1.

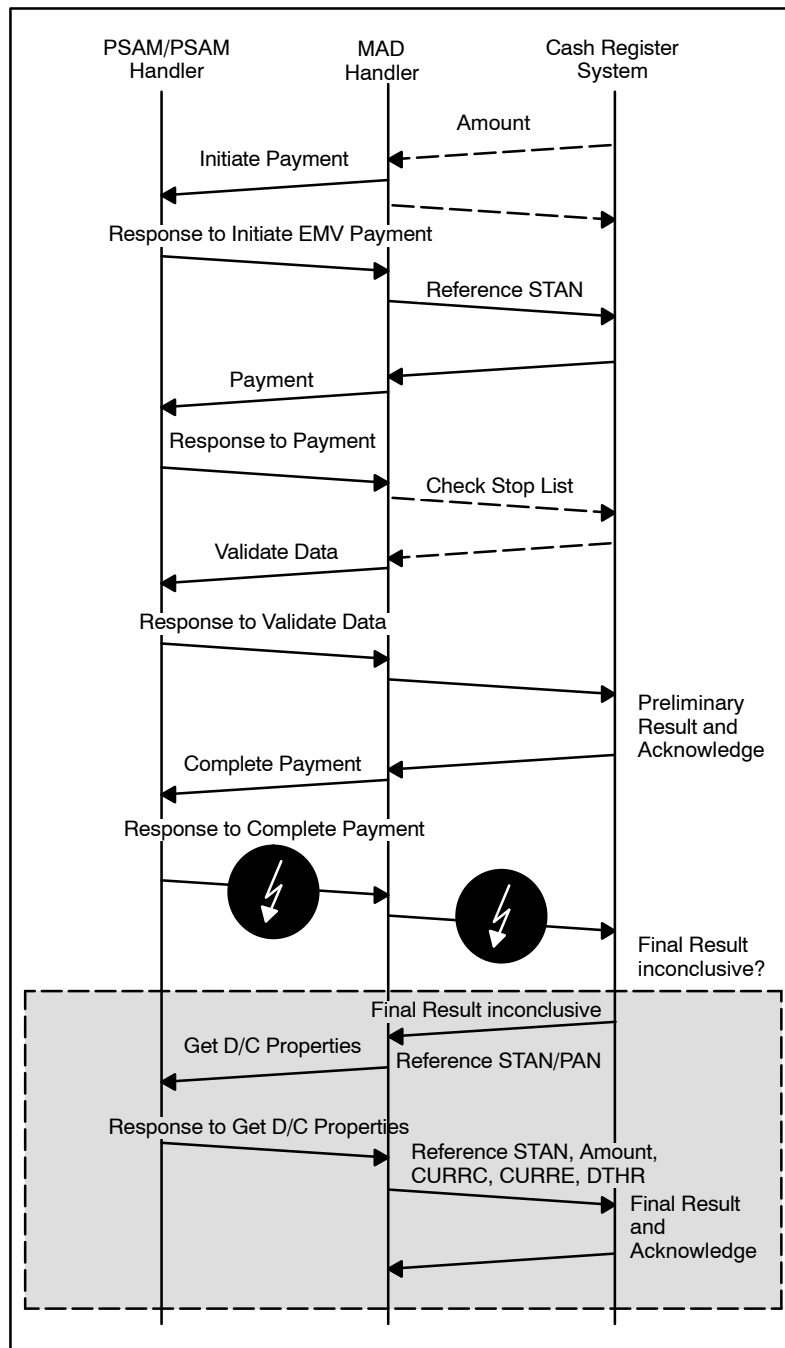


Figure 1-10.1 - Example of Command/Data Flow (Reference STAN)

PAN

If the Reference STAN is *not* known, the PAN may be used as search key instead.

NOTE: The use of the PAN as a search key is constrained by the PCI Security Requirements on the system.

At least two methods of using the PAN as search key are recognized:

1. The *Get Debit/Credit Properties* command may be issued, either based on the PAN stored earlier during the transaction, or based on key-entry of the PAN.
2. A new transaction may be initiated, *not* knowing if the new transaction shall be cancelled or continued. When the response to *Initiate Payment* command is available, the *Get Debit/Credit Properties* command is issued. Based on the response from this command, the terminal or cash register system (or the Merchant) shall decide whether the new transaction shall be cancelled or continued.

NOTE: Irrespective of the method used, the data returned from the PSAM shall be evaluated to ensure that the match is not an 'older transaction'.

1-10.7.5 Limitations

It is important to have the limitations described below in mind when designing systems using the status of the previous transactions.

Terminal Environments

The use of duplicate transaction check may not be suitable for certain unattended terminals, e.g. petrol stations and ticket vending machines. In these environments, the flow of a transaction may be as follows:

- A Preauthorization on a default amount is performed
- The goods are delivered
- A Capture is performed on the actual amount

As the default amount will be the same, duplicate transaction check is not to be performed on the authorization as this would inhibit the cardholder buying goods twice. Duplicate transaction check is for the same reason not activated on authorizations.

Duplicate transaction check on the Capture will generate an error if the customer makes a second purchase resulting in the same transaction amount. The authorization is completed with no check and the goods are handed over to the customer. However, the subsequent capture is declined, i.e. the customer gets the goods twice but only pays once.

Duplicate transaction check should be disabled in these environments. This is achieved by setting the time-out for the check to '0'. This is a local setting in the individual terminal.

Availability

The status of previous transactions is available when the terminal is either idle or between two command/response pairs e.g. after the response to the *Initiate Payment* command and before the *Payment* command.

Transaction Types

Only transactions with financial impact are logged. Data are logged only when one of the following Transaction Requests (TR) is indicated in the *Initiate Payment* command:

- Purchase (TR = '00')
- Refund (TR = '01')
- Capture (TR = '04')
- Post Purchase (TR = '0A')
- Post Refund (TR = '0B')

Approved/Successful Transactions

Only previous transactions which are considered as approved/successful by the PSAM (ASW1-ASW2 < '1100') will be logged by the PSAM.

Searching for a declined transaction in the *Get Debit/Credit Properties* command will result in a short response with an ASW1-ASW2 = '10 33' (Requested transaction not found).

Number of Entries

Currently, the number of entries in the PSAM log is limited to 8. It means that an approved transaction (number 9) will overwrite the oldest entry in the log.

NOTE: The actual number of entries may be changed without further notice.

NOTE: The value '00 00 00' is not a legal value for the Reference STAN.

PAN

Even though the PAN is logged and can be used as a search key, the PAN will *never* be revealed.

When the PAN is used as search key, the format i.e. the number of padding characters ('F') must be the same as indicated in the response to the *Initiate Payment* command.

When the PAN is used as search key, and the PSAM detects match for more than one transaction, only the result of the latest of these transactions is returned from the PSAM, i.e. the transaction with the highest STAN.

1-10.8 Contactless Transactions

1-10.8.1 Introduction

Contactless transactions are offered for the following card products:

PayPass (MasterCard)

The following AIDs are reserved for *PayPass*:

- MasterCard: 'A0 00 00 00 04 10 10'
- Maestro: 'A0 00 00 00 04 30 60'

PayPass supports two modes of operation:

- *PayPass* - Mag Stripe mode
- *PayPass* - *M/Chip* mode

PayWave - qVSDC (Visa)

The following AIDs are reserved for *payWave*:

- Visa Debit and Visa Credit: 'A0 00 00 00 03 10 10'
- Visa Electron: 'A0 00 00 00 03 20 10'

payWave supports one mode of operation:

- qVSDC – Quick Visa Smart Debit/Credit (ICC)

The terminal requirements for *PayPass* and *payWave* respectively are generally not identical. Furthermore, these card scheme specifications are updated independently of each other.

- 1-10.8.1.1 A The terminal vendor is responsible to keep updated with the requirements stated in the latest version of the MasterCard and Visa specifications for contactless transactions..

1-10.8.2 Kernel Configuration

Two distinct types of kernel configuration are defined:

- Internal kernel
- External kernel

Internal Kernel

The kernel is implemented in the PSAM. Internal kernel is currently not an available option!

External Kernel

For an external kernel solution, the terminal vendors is using approved kernels to interface to the PSAM.

The external kernel covers the solution where the terminal is conducting the transaction from:

- Pre-processing
- Contactless interface activation

- PPSE Selection
- Kernel processing (including CVM determination)
- Contactless interface deactivation

While the PSAM is responsible for CVM Processing, generating and storing the APACS messages.

- 1-10.8.2.1 A It is the task of the terminal vendor to comply with the requirements for a contactless terminal given by Visa and MasterCard. These requirements are not listed in this specification.

1-10.8.3 Contactless Transactions

The following transactions are applicable for contactless transactions:

- Purchase
- Refund
- Cashback
- Cancellation

Purchase

- 1-10.8.3.1 A Purchase (online/offline) is mandatory.

Refund

- 1-10.8.3.2 A In general, all attended POS terminals shall support contactless Refund transactions.

NOTE: Specific requirements may exist for *PayPass* and/or *payWave*.

Cashback

- 1-10.8.3.3 A Terminal supporting Purchase with Cashback shall provide a means by which this feature can be disabled.

- 1-10.8.3.4 A Cardholder verification (and online authorization) shall be performed for Purchase with Cashback transactions.

- 1-10.8.3.5 A Purchase with Cashback shall not be performed for *Maestro PayPass*.

NOTE: Specific requirements may exist for *PayPass* and/or *payWave*.

Cancellation

- 1-10.8.3.6 A All attended POS terminals shall support Cancellation of contactless Purchase transactions.

NOTE: The special requirements for contactless transactions are handled by the PSAM in the background.

1-10.8.4 Transaction Flow - External Kernel

Six commands are defined between the terminal and PSAM:

During start-up:

These commands are issued during the start-up process and do therefore not influence the transaction time.

- **Get CA Public Key Information.** This command is used to convey required key information from the PSAM to the terminal in the response.
- **Get Contactless AID related Information.** This command is used to convey required information concerning limits, Application Program ID etc. from the PSAM to the terminal in the response.
- **Get Tag List for External Kernel.** This command is used to convey requested data elements required by the PSAM to generate the messages to the host. The PSAM will return a tag list. This tag list is generic for all transaction types.

The already defined commands used during start-up such as e.g. *Start-up PSAM*, *Get Debit/Credit File Characteristics* and *Configure PSAM Application* are still applicable. See figure 1-10.2 below.

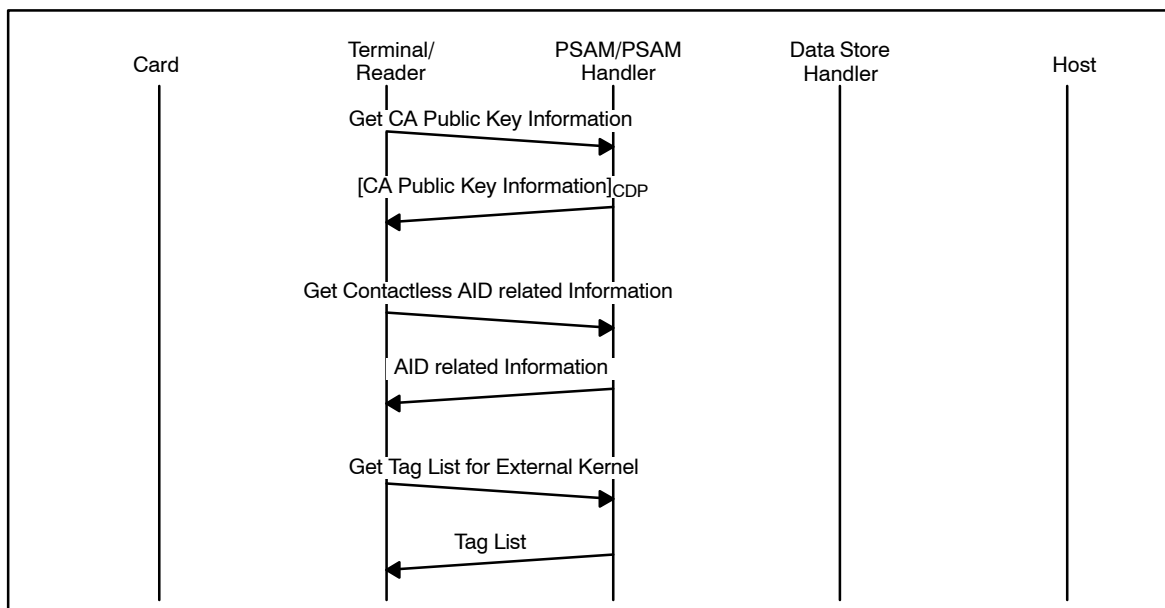


Figure 1-10.2 - Contactless Transaction (Start-up)

During the transaction:

- **Initiate Contactless Payment.** This command is issued upon completion of the kernel processing and initiates the CVM handling (if required) and the subsequent generation of an APACS60 message (either an Authorization Request or a Financial Advice). All the data elements required for the receipt will be returned in case of an offline transaction. For an online transaction, some of the data elements required for the receipt will be returned.
- **Validate Contactless Payment.** This command is used to convey the host response to the PSAM. Remaining data elements required for the receipt printing will be returned.
- **Complete Contactless Payment** The terminal will indicate in this command whether the transaction is to be considered successful or not. The Advice will be saved in Data Store.

- 1-10.8.4.1 A The Transaction Sequence Counter is not provided by the PSAM before the transaction. If the card requests the Transaction Sequence Counter (tag '9F41') the terminal shall be able to generate it. The Transaction Sequence Counter will be conveyed in field 55 to the host.

NOTE: The PSAM will return the STAN to be printed on the receipt.

Offline Transactions

- 1-10.8.4.2 A For offline contactless transactions, only the following commands shall be issued:

- *Initiate Contactless Payment*
- *Complete Contactless Payment*

The response of the Initiate Contactless Payment command will return the necessary for the terminal to act on (receipt etc.)

Online Transactions

- 1-10.8.4.3 A For online contactless transactions, the following commands shall be issued:

- *Initiate Contactless Payment*
- *Validate Contactless Payment*
- *Complete Contactless Payment*

NOTE: The contactless commands are defined in section 2-14, "Commands and Responses".

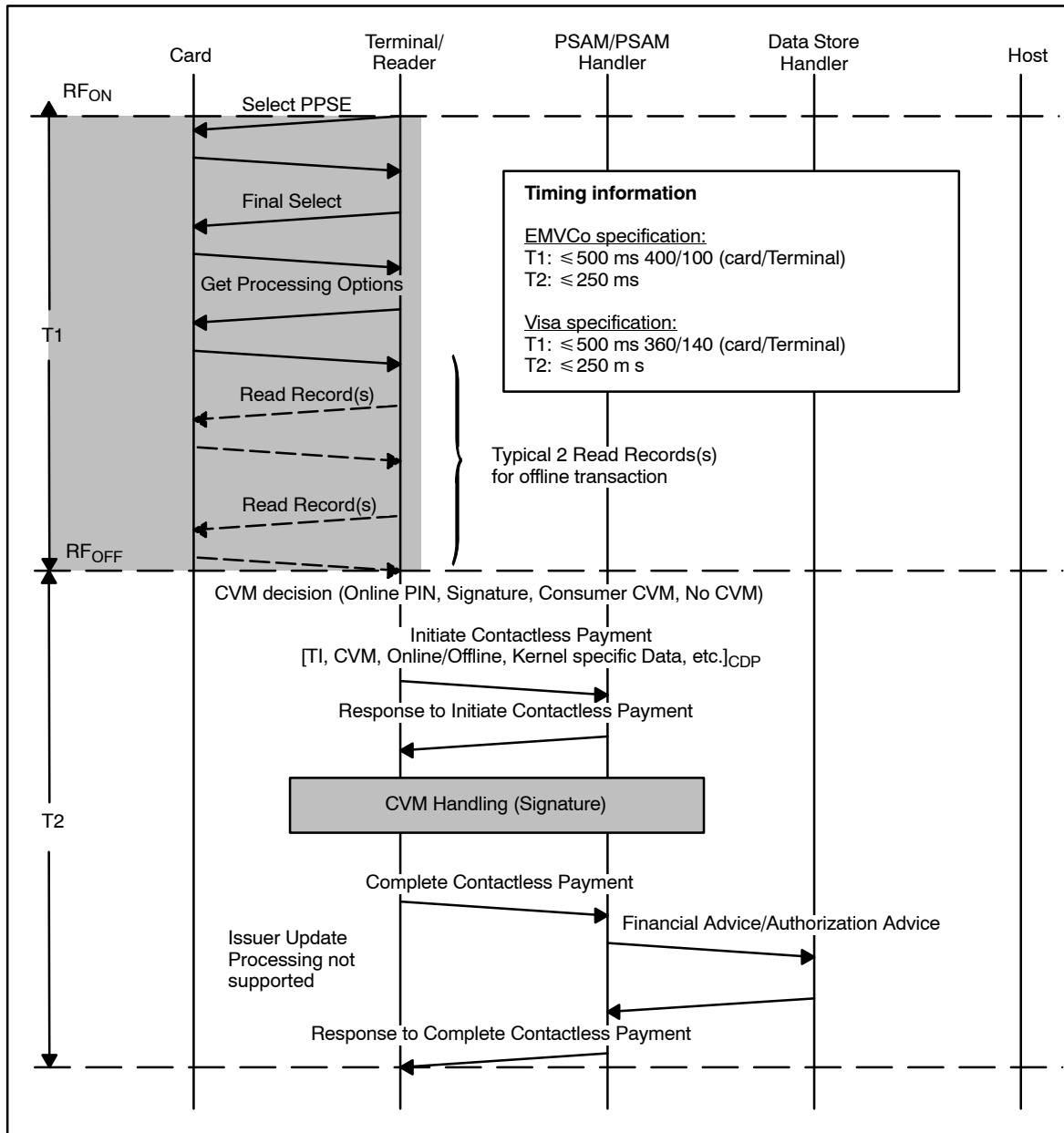


Figure 1-10.3 - Visa payWave (qVSDC) - Offline

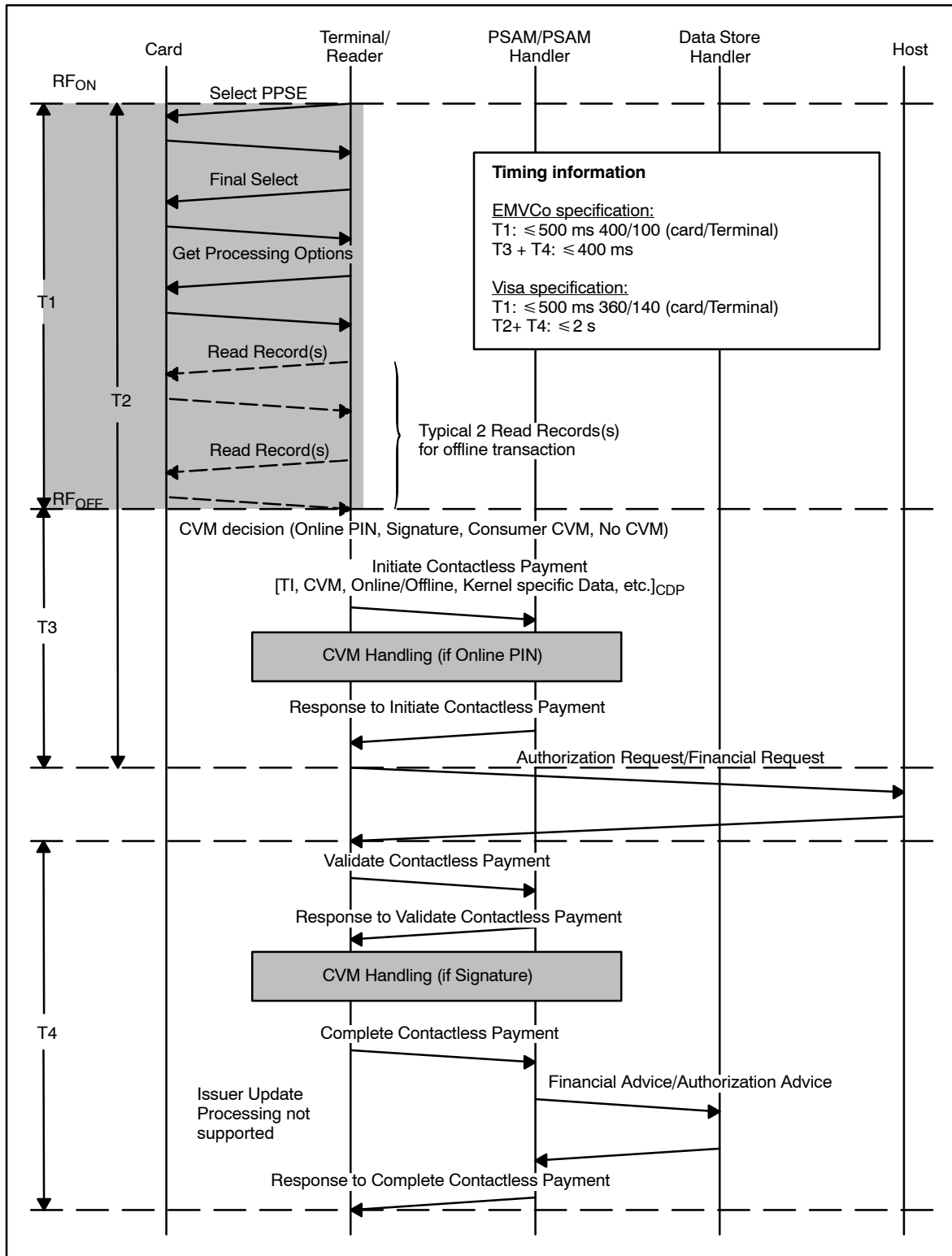


Figure 1-10.4 - Visa payWave (qVSDC) - Online

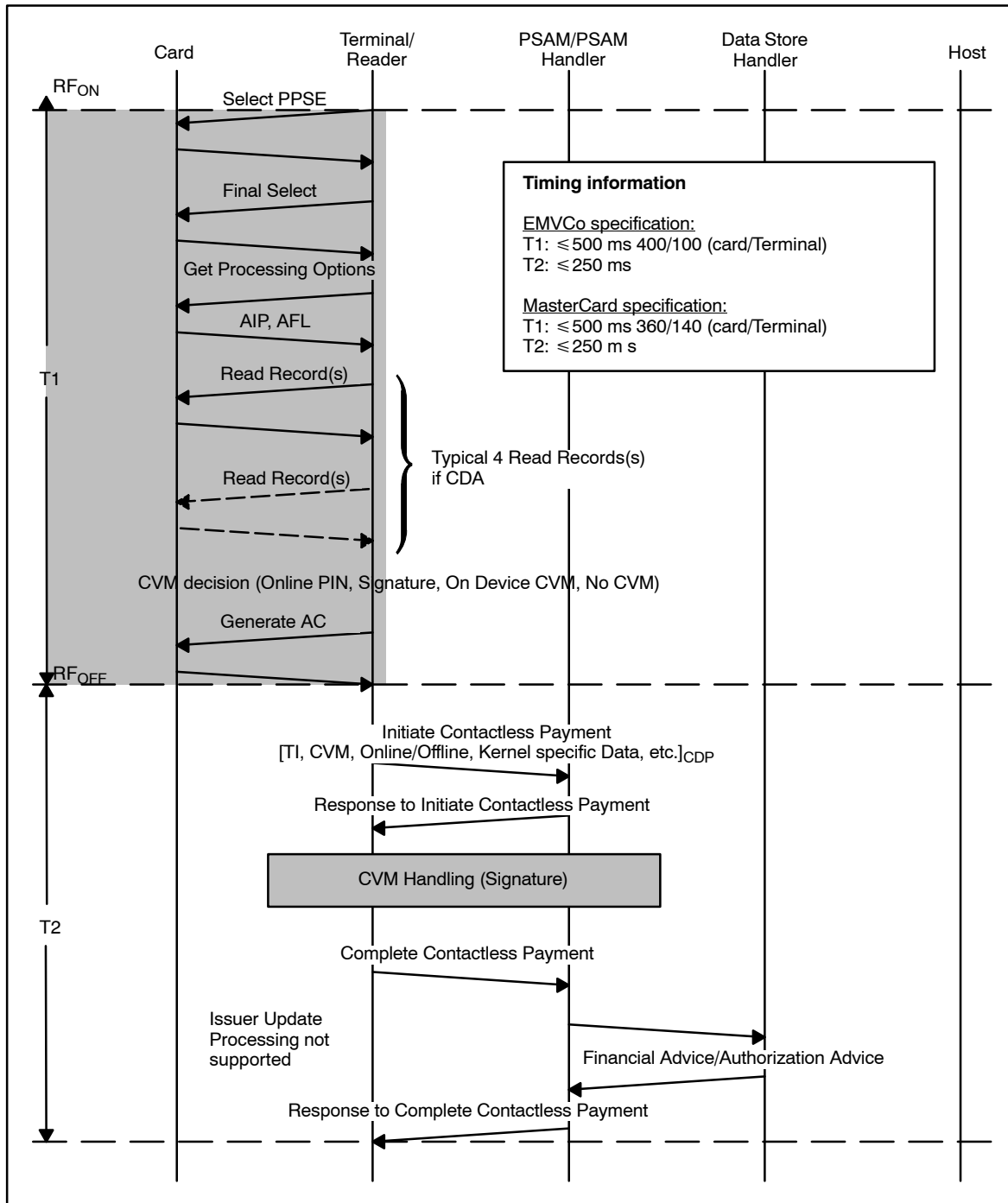


Figure 1-10.5 - MasterCard PayPass - Offline

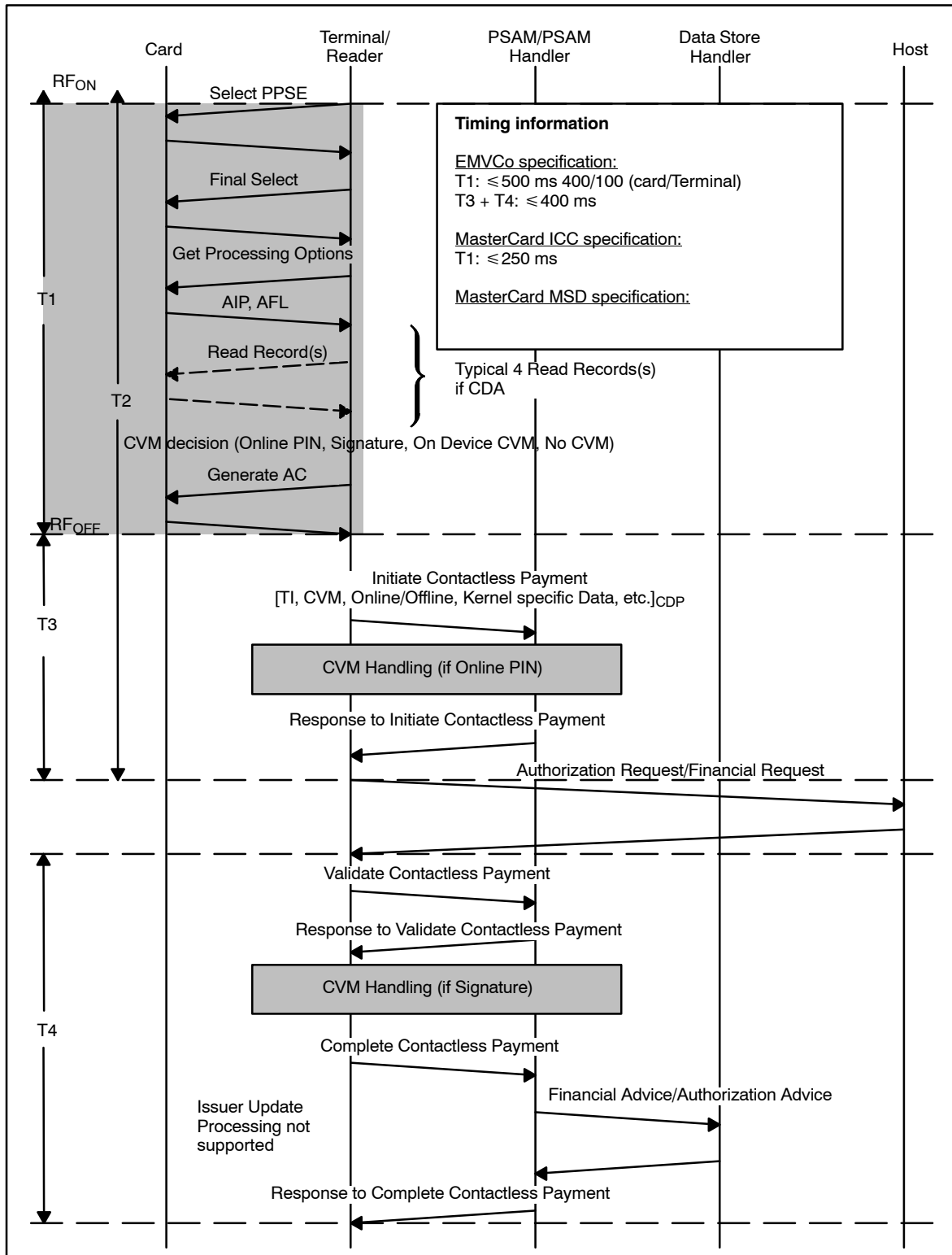


Figure 1-10.6 - MasterCard PayPass - Online

1-10.8.5 Rejected/Declined Transactions

Terminal – PSAM interface signalling

The external kernel may decide that the transaction should be either rejected or declined while the kernel is in charge.

In this case the kernel will deliver specific “error codes” explaining the reason for rejection or declining. It is important that these error codes are forwarded to the host, where they can be used for diagnostic or statistic purposes.

- 1-10.8.5.1 A A general rule is, when the external kernel has been initiated, the PSAM shall generate an APACS message.

NOTE: If the transaction fails before an AID or Kernel ID is obtained, there is no reason for initiating the PSAM.

So despite the outcome of the kernel processing (successful, declined, use another interface etc.), the PSAM shall be initiated.

Fallback to other technology

- 1-10.8.5.2 A If a contactless transaction does not successfully complete for any reason other than a communication error, and then the terminal should prompt for a contact transaction to be performed. It should not be assumed that the same card will be declined when used in contact profile.

Preferences:

- Contact EMV
- Magnetic stripe (swipe)

- 1-10.8.5.3 A payWave rules for fallback to other technology shall be in accordance with ref. 41: “Visa Contactless Payment Specification (VCPS), Version 2.1, May 2009” (and updates), section 5.13.

Table 1-10.7 - *PayPass* Fallback Rules

Terminal – Action Indicator	PSAM	Host	ASW1–ASW2
Approved	Approved	Approved	‘0000’
Approved	Approved	Declined	‘10FC’
Approved (On Device Cardholder Verification)	Approved	Declined	Non ‘10FC’
Approved (Not On Device Cardholder Verification)	Rejected	–	‘10FC’
Approved (On Device Cardholder Verification)	Rejected	–	Non ‘10FC’
Declined, unconditional	Declined	–	Non ‘10FC’
Declined, new technology recommended	Declined	–	‘10FC’

Table 1-10.8 - *payWave* Fallback Rules

Terminal – Action Indicator	PSAM	Host	ASW1–ASW2
Approved	Approved	Approved	‘0000’
Approved	Approved	Declined	Non ‘10FC’
Approved (Not Consumer Device CVM)	Rejected	–	‘10FC’
Approved (Consumer Device CVM)	Rejected	–	Non ‘10FC’
Declined, unconditional	Declined	–	Non ‘10FC’
Declined, new technology recommended	Declined	–	‘10FC’

Error Codes

- 1-10.8.5.4 A Whenever the terminal/External Kernel encounter an error, the terminal map this incident to an Error Code value.

Applicable Error Code values can be found in section 2-15.2.56.

1-10.8.6 Protection against Replay Attacks

The response to the *Complete Contactless Payment* command is protected against replay attack. This is accomplished by using the session key $KSES_{CDP}$ the following way:

- The “seed” (4 bytes) is generated,
- Random data, 4 bytes, is concatenated leading the input data of the *Initiate Contactless Payment* command,
- The concatenated data are “padded” the ISO way, i.e. always padding with a 1 bit and a number of 0 bits until a 8 byte boundaries,
- $KSES_{CDP}$ is generated,
- Random, Data and Padding is encrypted using 3DES and CBC,
- The seed is inserted in front of the encrypted data,
- The length is calculated over the full size of data.

For the *Initiate Contactless Payment* command, an additional random number (Transaction Identifier) is generated by the terminal.

- 1-10.8.6.1 A The terminal shall never generate a Transaction Identifier where all the bits are set to zeroes in the *Initiate Contactless Payment* command.

This random number is part of the enciphered data sent to the PSAM and is returned (enciphered) in the final response to the terminal (which response is depending on whether the transaction has been performed on or offline).

The PSAM will then check the Transaction Identifier (in clear text) conveyed in the *Complete Contactless Payment* command. If identical with the previously given value, the transaction will continue.

The PSAM will detect (using Transaction Identifier and DTHR) that the same commands are not replayed.

1-10.8.7 CVM Handling

General considerations

It is the external kernel that makes the decision of which CVM has to be performed. This decision is forwarded to the PSAM using the data element “Action Indicator” in the *Initiate Contactless Payment* command. The security zone established between the terminal and PIN Pad is used if the decision requires online PIN. If signature is the final decision, the signing takes place just before the *Complete Contactless Payment* command where the receipt is available. It is possible for the merchant to reject the transaction if e.g. the signature cannot be approved by setting parameters in the *Complete Contactless Payment* command.

The following CVMs are supported/accepted (Visa/Master-Card):

- Online PIN
- Consumer Device CVM/On Device Cardholder Verification

- Signature

Consumer Device CVM/On Device Cardholder Verification

The terminal shall support Consumer device CVM (Visa term)/ On Device Cardholder Verification (MasterCard term).

Consumer device CVM

- 1-10.8.7.1 A When a consumer device indicates to the reader that consumer interaction is required in order to allow the transaction to progress, the reader shall:
- Power down the contactless interface
 - Indicate to the cardholder to refer to their device for further instructions. E.g. "See phone for instructions"
 - Extinguish the status indicators
 - Sound the alert tone

NOTE: The consumer's device indicates that consumer interaction is required by responding to *GET PROCESSING OPTIONS* with SW1 SW2 = '6986'.

- 1-10.8.7.2 A For Contactless mobile payment, the data element Merchant Name and Location (tag '9F4E') shall contain the merchant's name as known to the general public and a location that is meaningful to the cardholder. The terminal shall return the value of the Merchant Name and Location when requested by the card in a Data Object List. A consumer device will typically only request the first 20 characters of this data.

Contactless mobile payment retrieve this data element and record it as part of the transaction data displayed to the cardholder on the handset.

NOTE: The information can be obtained from the *Merchant Static Data Information* (Update tag '0014').
ME_{NAME} (18 bytes) and ME_{ADDRESS} (24 bytes). The terminal strips of any spaces.

On Device Cardholder Verification

- 1-10.8.7.3 A When the On Device Cardholder Verification is recognized, the transaction shall be terminated and a new transaction is initiated after the secret code has been entered on the device.

PIN-retry

PIN-retry is not supported for contactless transactions.

1-10.8.8 Contactless Limits

For contactless transactions the following limits are defined:

- **Reader Contactless Floor Limit.** Indicates the floor limit in the terminal.
- **Reader CVM Required Limit.** Indicates the CVM limit of the reader for an application. If the transaction amount is greater than or equal to the Reader CVM Required Limit, then the reader requires a CVM for the transaction.

- **Reader Contactless Transaction Limit.** Indicates the contactless transaction limit of the reader for an application. If the transaction amount is greater than or equal to the Reader Contactless Transaction Limit, then a contactless transaction is not permitted. Switching the transaction over to another interface is permitted.

NOTE: *payWave* allows contactless transactions below the Reader Contactless Transaction Limit regardless of the CVM. Contactless transactions are still allowed above this limit, but only if a CVM is used (that is, the cardholder is verified). Default requirements for contactless limits: Reader CVM Required Limit = Reader Contactless Floor Limit. Reader Contactless Transaction Limit is not used.

PayPass operates with two additional limits:

- **Soft limit**—refers to implementations where transactions over a given value require cardholder verification.
- **Hard limit**—refers to implementations where a maximum transaction amount is set and cardholder verification is never required below this limit.

NOTE: Note that contactless transactions for a given AID are always performed in the currency returned in the response to the *Get AID related Information* command for this AID and all limits refer to this currency. It is the task of the terminal to limit the number of currencies.

The card may internally convert this transaction currency to the card domestic application currency, if supported.

The configuration of *PayPass* - M/Chip limits results in one of these implementation types within a region or market.

1-10.8.9 Application Program ID

Contactless Reader Limits allow the reader to support multiple sets of reader risk parameters. For *payWave* the reader determines which limits apply to a particular transaction by examining the Application Program ID (tag '9F5A'), provided to the reader in the Issuer Discretionary Data (tag 'BFOC') of the application's SELECT response. The limits will be defined with the merchant and the issuer carrying the specific Application Program ID.

Contactless Reader Limits can be merchant specific. It is essential that the number of Contactless Reader Limits are flexible i.e. easy to add or delete rows.

- | | | |
|------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.8.9.1 | A | <p>The terminal shall be able to hold at least 4 (additional) Reader Limit Sets (each set consists of up to 32 bytes)</p> <ul style="list-style-type: none"> • LEN_{RAPI} (1 byte) • RAPI (1 - 16 bytes) • Currency (3 bytes) • Reader Limit Set (12 bytes) |
|------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1-10.8.10 Restrictions for Contactless Transaction

Dynamic Currency Conversion (DCC)

Dynamic Currency Conversion (DCC) is not available for contactless transactions as the final amount shall be present at the beginning.

Token based Transactions

Token based transactions are not supported for contactless transactions.

Surcharge/Gratuity

Surcharge is not possible as the PAN is not available when the final amount is to be calculated.

If gratuities are to be included in the contactless transaction then the cardholder should be offered the opportunity to add the gratuity amount before the contactless transaction commences.

1-10.8.11 Optional Functions

Issuer Envelope Data/Extended Issuer Envelope Data

Issuer Envelope Data and Extended Issuer Envelope Data are applicable when performing contactless transactions if the following rules are fulfilled:

- Data to be conveyed in the Authorization Request/Financial Request (online) shall be presented (using a *Set Debit/Credit Properties* command) before the *Initiate Contactless Payment* command.
- Data to be conveyed in the Financial Advice shall be presented (using a *Set Debit/Credit Properties* command) before the *Complete Contactless Payment* command.

Loyalty

In the response to *Select* command, a Nets Proprietary Data Element has been defined inside the FCI Issuer Discretionary Data. The tag and value are yet to be defined, but it will be in the range 'DFxx'. It will be the task of the terminal to recognise this tag.

1-10.9 Prepaid MSC Transactions

1-10.9.1 Functional Requirements

- 1-10.9.1.1 B A terminal supporting Prepaid MSC functionality shall implement 'Pay with a Prepaid MSC'.
- 1-10.9.1.2 B A terminal supporting 'Pay with a Prepaid MSC' shall implement 'Balance Inquiry on a Prepaid MSC'.
- 1-10.9.1.3 C A terminal supporting Prepaid MSC functionality may implement 'Load a Prepaid MSC'.
- 1-10.9.1.4 C A terminal may support 'Offline Pay with a Prepaid MSC' and 'Offline Load of a Prepaid MSC'.
- 1-10.9.1.5 A A 'Balance Inquiry on a Prepaid MSC' shall generate an Authorization Request with an amount of 0,00 in the merchants local currency. The Prepaid MSC account balance and expiration date is returned in the Authorization Request Response.
- 1-10.9.1.6 A The Token returned to the terminal shall be discarded by the terminal or the cash register, since the Token is not used in a succeeding 'Pay with a Prepaid MSC'.
- 1-10.9.1.7 C The process of paying with a Prepaid MSC should consist of two parts, a 'Balance Inquiry on a Prepaid MSC' followed by a 'Pay with a Prepaid MSC'. The terminal may combine the two parts of the payment process into a single operation.
- NOTE:** A 'Pay with a Prepaid MSC' should only be initiated (by the merchant) if sufficient funds are available for performing the purchase.
- NOTE:** The handling of split payment, i.e. partial payment with the prepaid MSC is expected to be handled by the Cash Register and is outside the scope of the terminal. The terminal will only see the individual card transactions.
- 1-10.9.1.8 A The 'Pay with a Prepaid MSC' shall generate a Purchase business call (a standard Financial Request). The Prepaid MSC account balance and expiration date is returned in the Financial Request Response.
- 1-10.9.1.9 C The process of loading a Prepaid MSC should consist of two parts, a 'Balance Inquiry on a Prepaid MSC' followed by a 'Load a Prepaid MSC'. The terminal may combine the two parts of the loading process function into a single operation.
- 1-10.9.1.10 B A 'Load of a Prepaid MSC' shall generate a Refund business call (a standard Financial Request) to transfer the funds to the card. The Prepaid MSC account balance and expiration date is returned in the Financial Request Response. The funds transfer shall be performed online to enable the cardholder to use the card immediately.
- 1-10.9.1.11 A The 'Offline Pay with a Prepaid MSC' function is performed when a online connection is not possible. It shall consist of an offline Purchase business call. The Financial Advice generated will be stored in the terminal Data Store for later transfer to the Host.
- NOTE:** The procedure is that the merchant should retain the card after an 'Offline Pay with a Prepaid MSC'

has been performed, i.e. a transaction is performed on the supposed remaining balance. It is the responsibility of the merchant to ensure that the card is retained after an 'Offline Pay with a Prepaid MSC' has been performed.

- 1-10.9.1.12 A The 'Offline Load of a Prepaid MSC' is performed when an on-line connection is not possible. It shall consist of a Refund business call performed offline. The Financial Advice generated will be stored in the terminal Data Store for later transfer to the Host.

NOTE: The consequence is that the cardholder cannot use the card immediately. It is the responsibility of the merchant to inform the cardholder that the card cannot be used before the following day, at the earliest.

NOTE: 'Offline Load of a Prepaid MSC' should not be performed for non-empty cards.

It is the responsibility of the merchant to observe the current regulations with regards to any Prepaid MSC balance.

It is always the cash register that determines the Amount and the Track2 Data to be used with any Business Call initiated from the cash register.

- 1-10.9.1.13 A When a business call is initiated, the cash register shall include an Amount and Track2 Data in the call to the terminal.

1-10.9.2 Host Data Transfer

A terminal used only for Prepaid MSCs need not support any specific service packs in order to handle Prepaid Cards. Accelerated PIN Entry (APE) and Dankort Accelerated PIN Entry (DAPE) may or may not be supported by the terminal.

It is not necessary to send any specific Prepaid MSC information to the Host.

- 1-10.9.2.1 A The terminal shall, when performing Prepaid MSC transactions, analyze the host response in order to extract Prepaid MSC specific information. The necessary Prepaid MSC information is conveyed to the terminal in the Host responses, i.e. in the Authorization Request Responses and Financial Request Responses.

The general description of the response from the Host is found in section 2-13, "Host Communication for the Debit/Credit Application - Protocols and Formats".

- 1-10.9.2.2 A The terminal shall, when Prepaid MSC information is returned in the response from the Host, retrieve the information from field 44. The Issuer Envelope Response Data, tag TY holds the information.

Under tag TY two tags are defined:

- Tag E6 - Balance/Available funds
- Tag M4 - Expiration date for the available funds

The format of the tags is specified in table 1-10.9.

Table 1-10.9 - Format of Tag E6 and M4

Tag	Item	Size	Attributes
E6	Balance/available funds	6 bytes	n12
M4	Expiration date for the available funds	2 bytes	n4

Tag E6 holds the balance/available funds in the minor unit of the currency.

Tag M4 holds the expiration date in the format YYMM

Example: A balance of 1234,56 with an expiration date of 2009 January is coded as;

54 59 00 10 45 36 00 06 00 00 00 12 34 56 4D
34 00 02 09 01

- 1-10.9.2.3 A The terminal shall, when performing an offline Business Call substitute the response from the Host with blank data.

The requirements for receipts from a Prepaid MSC transaction can be found in section 1-12.

1-10.9.3 Prepaid MSC Transaction Flow

The section below details the overall flow of the different Prepaid MSC functions

Balance Inquiry

The flow of 'Balance Inquiry on a Prepaid MSC'

- The merchant swipes or scans the Prepaid MSC
- Balance Inquiry is initiated in the cash register
- The terminal initiates an Original/Extended Authorization
- The balance returned indicates the funds available on the Prepaid MSC.
- The terminal or the cash register discards the Token issued.
- A Receipt with the balance is printed.

Paying with a Prepaid MSC

The flow of 'Pay with a Prepaid MSC'

- The merchant initiates and completes a Balance Inquiry
- If the balance returned indicates that sufficient funds are available on the Prepaid MSC, a Purchase is initiated.
- The terminal initiates a Purchase with the Amount and Track2 Data from the cash register.
- Purchase completed OK.
- A Receipt with actual balance is printed.

Loading a Prepaid MSC

The flow of 'Load a Prepaid MSC'

- The merchant initiates and completes a Balance Inquiry
- ~~If the balance returned indicates that the card account is 'empty', the merchant initiates a Load a Prepaid MSC in the cash register.~~

NOTE: It is no longer necessary that the 'account' is empty before loading.

- The terminal initiates a Refund with the Amount to be loaded onto the Prepaid MSC using Track2data from the cash register.
- The balance returned indicates the funds available on the Prepaid MSC.
- Load completed OK
- A receipt with actual balance printed.

Paying with a Prepaid MSC, Offline

The flow of 'Offline Pay with a Prepaid MSC'

- The merchant initiates a Balance Inquiry.
- If no response is received, the Merchant may decide to initiate and complete a 'Offline Pay with a Prepaid MSC' in the cash register.
- The cardholder states an expected balance. The attendant can then choose to trust the cardholder. The attendant will however usually perform an Offline Purchase on the full expected balance, and retains the Prepaid MSC after the transaction has taken place.
- Terminal initiates an Offline Purchase with the Amount and Track2Data received from the cash register.
- Purchase completed OK.
- A Receipt where a blank balance is printed.
- The Financial Advice is sent to Nets Denmark A/S when possible.

Loading a Prepaid MSC, Offline

The flow of 'Offline Load a Prepaid MSC'

- The merchant initiates a Balance Inquiry
- If no response is received, the Merchant may decide to initiate and complete a 'Offline Load a Prepaid MSC' in the cash register.
- It is the responsibility of the merchant to inform the cardholder that the card, at the earliest, may be used the following day.
- The terminal initiates an Offline Refund with the Amount to be loaded onto the Prepaid MSC using Track2data from the cash register.
- Load completed OK
- A Receipt where a blank balance is printed.
- The Financial Advice is sent to Nets Denmark A/S when possible.

1-10.9.4 Error Situations

For specific handling of advices, see section 2-5.15

Declined Transactions

- | | | |
|------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.9.4.1 | A | The terminal shall print the Balance and Expiry Date on the receipt if the information has been provided in the response from the Host, otherwise these fields shall be blank. |
| 1-10.9.4.2 | C | The terminal may, for a declined operation, append supplementary information to the receipt. |

1-10.9.5 Entry of PAN Information

This section handles the entry of PAN information using the magnetic stripe or the optional bar code on the card.

Using magnetic stripe

When the magnetic stripe is used, the procedure is as follows.

- 1-10.9.5.1 A When the magnetic stripe is swiped in a separate magnetic stripe card reader on the cash register, the cash register shall forward the Track2 Data to the terminal. The terminal shall then process the transaction as any other transaction with the exception of printing the additional Prepaid MSC information on the receipts.

- 1-10.9.5.2 A If the magnetic stripe card reader on the terminal is used, the terminal shall process the transaction as any other transaction with the exception of printing the additional Prepaid MSC information on the receipt.

A specification of the format of Prepaid MSC PAN is given in table 1-10.10.

Table 1-10.10 - Primary Account Number

Position	Description	Value
1	National use	9
2 – 4	Country code (see NOTE)	208
5	Type – financial application	6
6 – 8	Nets id (See NOTE)	075
9 – 11	Customer number	1–999
12 – 18	Serial number	1–9999999
19	Check digit modulus 10, Luhn formula	0–9

NOTE: The country code and institution ID listed is for Nets in Denmark. Country codes are specified in ref. 1: "ISO 4217". Institution ID is allocated nationally.

An example of a Prepaid MSC PAN is;

9 208 6 075 100 0000001 1

Using Bar Code

This section describes the construction of the PAN, when data is gathered by scanning the bar code on the Prepaid MSC.

- 1-10.9.5.3 A When the bar code on the Prepaid MSC is scanned, special functionality on the cash register or in the terminal shall use the information gathered to construct Track2 Data that can be used to perform the actual transaction.

The format of data received from the scanned bar code on a Prepaid MSC is given in table 1-10.11.

Table 1-10.11 - Scanned Bar Code Data

Position	Description	Value
1 – 15	Digits 5–19 of the Primary Account Number	1–999999999999999
16 – 19	To be used in the constructed magnetic stripe	1–9999

An example of data gathered from the scanning of a bar code of a Prepaid MSC is;

6 075 100 0000001 1 4711

1-10.9.5.4

A When Track2 Data shall be constructed from data received from the scanning of a Prepaid MSC, the following shall apply;

1. The 4 right hand digits of the data obtained from the scanning of the bar code of a Prepaid MSC shall be removed and stored for later use in step 6,
2. The digits 9xxx shall be added as the 4 left hand digits, where xxx is country code according to ref: 1 "ISO 4217".
3. The constructed Primary Account Number is now available,
4. On the right hand side of the constructed Primary Account Number a Separator shall be added,
5. The digits 4912702000000 shall be added to the right of the Separator,
6. The 4 stored digits shall be added as the final right hand digits,
7. The constructed Track2 Data is now ready to be used,

Example:

1. 6075100000000114711 Ⓢ
607510000000011
2. 607510000000011 Ⓢ
920860751000000011
3. 920860751000000011
4. 9208607510000000011 Ⓢ
920860751000000011D
5. 9208607510000000011D Ⓢ
9208607510000000011D4912702000000
6. 9208607510000000011D4912702000000 Ⓢ
9208607510000000011D49127020000004711
7. 9208607510000000011D49127020000004711

As the terminal shall strip the Start Sentinel, the LRC and the End Sentinel from any magnetic stripe sent to the PSAM, this shall not be included in the construction of Track2 Data.

The coding of Track2 Data is defined in section 2-15.2.154.

1-10.10 Loyalty information

1-10.10.1 Introduction

Certain issuers include loyalty information in their card data. This is the case for MSC as well as ICC. The PSAM is

enhanced to be able to provide such data to the terminal. This can be performed after the card has been read and before the transaction is initiated. The PSAM ensures that no PCI sensitive information is revealed.

- 1-10.10.1.1 A The terminal shall implement and use Cardholder Data Protection (CDP) to be able to use the commands. The following commands are introduced:

- *Retrieve Card Data* (with MSC data)
- *Retrieve Card Data* (with ICC data)

An overview of the command is given below.

NOTE: A terminal without CDP will be able to access the information directly.

1-10.10.2 Using MSC cards

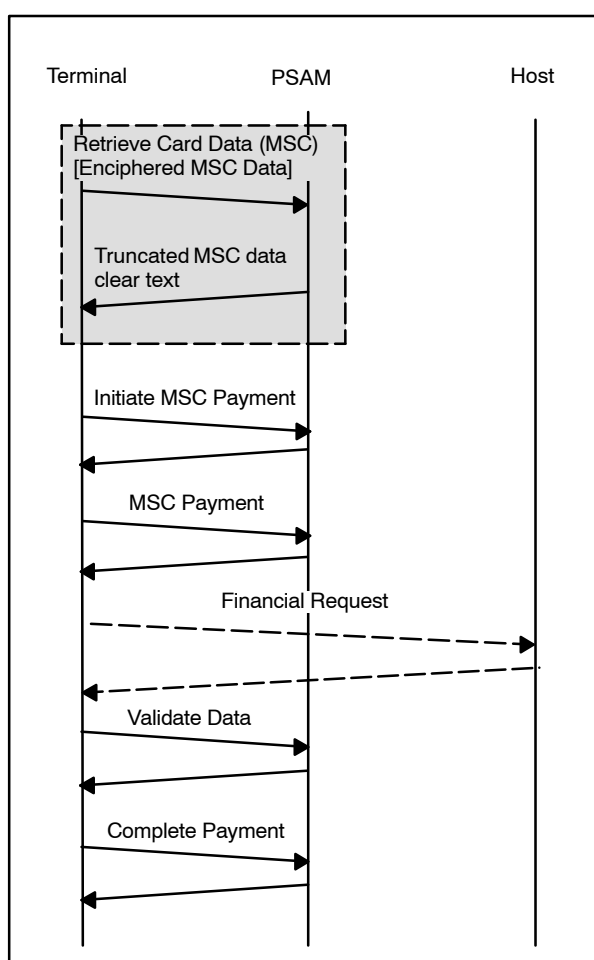


Figure 1-10.7 - Example of Retrieve Card Data (MSC)

The flow of the command for MSC is as shown in Figure 1-10.7 above. The detailed information on the command is given in section 2-14.6.26. The command uses a seed and the enciphered track data as input. The CDP enciphered data for all three tracks may be provided. The seed is included to protect against man-in-the-middle attacks. The output depends on whether or not the card is a Private Label card. The PSAM will for Private Label cards return the track information in plain text. It will for non-Private Label cards return the track data in masked format.

1-10.10.3 Using ICC cards

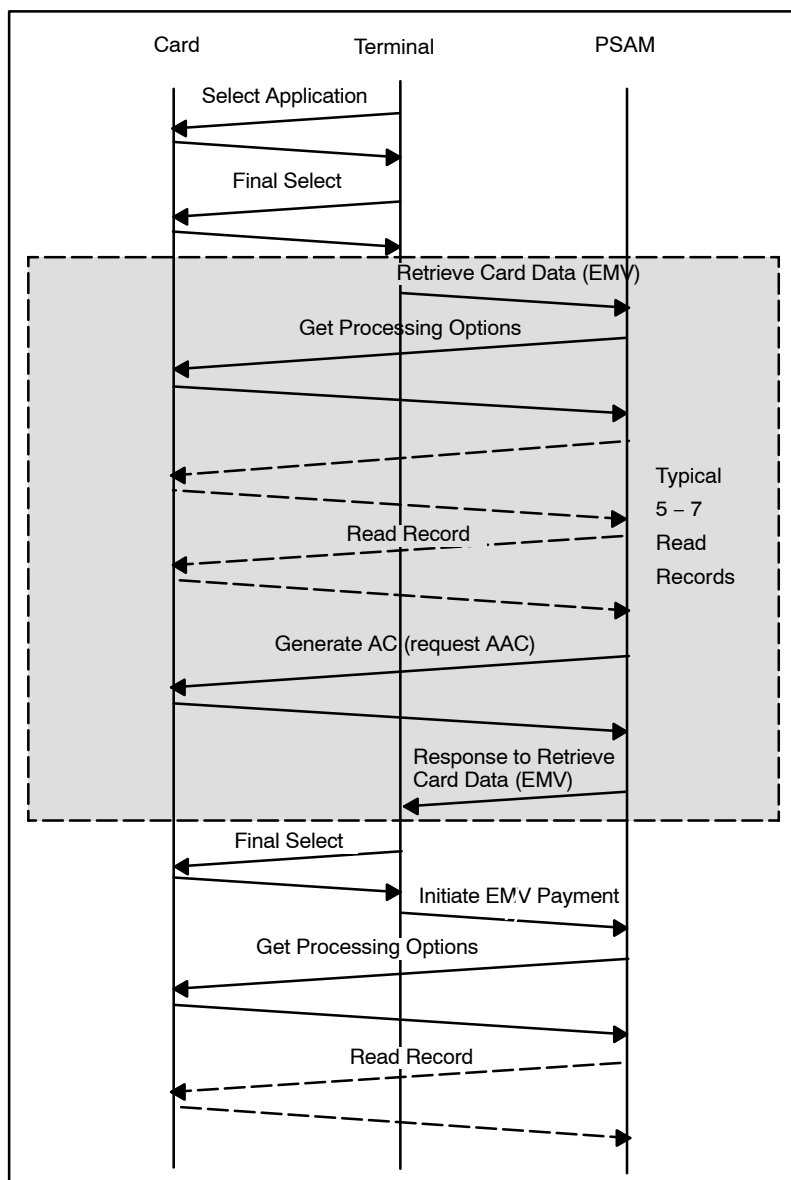


Figure 1-10.8 - Example of Retrieve Card Data (ICC)

The flow of the command for ICC is as shown in Figure 1-10.8 above. The detailed information on the command is given in section 2-14.6.27. The command uses a request with a Tag List. The command shall as well include an amount and a currency to take into account that the card may request these data in PDOL.

The command will return the requested data in TLV format. The PSAM will, based on the Application PAN in the card, check if the card is a Private Label card. The PSAM will return unmasked data if this is the case. The PSAM will, if the card is a non-Private Label card i.e. a PCI card, mask the data, as specified in 1-10.10.5 .

1-10.10.4 Expiration Date

There is a special issue with respect to Expiration Date handling. Expiration Date is in PCI scope. The check is thus

for PCI cards performed internally by the PSAM and only the result of the check is revealed.

The PSAM will for an ICC, if the card is in PCI scope, return an ASW1-ASW2 of '1095' if the card is expired. This is independent of whether or not tag '5F24' was requested.

The PSAM will, for a MSC card, return a Card Service Info indicating whether or not the card is expired. The format of the Card Service info is found in 2-15.2.31.

The PSAM will not perform any Expiration Date check for Private Label cards as the terminal has access to the data in clear text.

1-10.10.5 Masking of data

Data will be masked if the card is a valid PCI card and the data is within PCI scope. The rules for the different data elements follows below.

Track1

Track1 data is recognized to be in accordance with ISO/IEC 7813 if:

- There are up to 79 alphanumeric characters (76 in command),
- The Format code is "B", '22',
- There are no illegal character(s) in the PAN,
- The PAN is in the range 8 – 19 digits.

Track 1 will be left unmasked if;

- The track1 data are *not* recognized to be in accordance with ISO/IEC 7813, or
- The track1 data are recognized to be in accordance with ISO/IEC 7813 and it is indicated as Private Label Card.

Track 1 will be masked as;

- Cardholder Name will be masked to "<spaces>/<spaces>",
- PAN will be masked with "A", i.e. '21' for raw data format and '41' for full ASCII format. The masking is according to PCI rules (6 + 4 digits unmasked). See Table 1-12.4,
- Service code will be masked with "AAA",
- Expiration Date will be masked with "AAAA"
- PIN Verification Data will be masked with "AAAAA".

Track 2

Track2 data is recognized to be in accordance with ISO/IEC 7813 if:

- There are up to 40 decimal digits / separators (37 in the command),
- The PAN is in the range 8 – 19 digits, with no illegal characters,
- If there are 2 separators in the string, then they must be placed next to each other "=", or they must be placed with 4 digits in between "=nnnn=",
- If there are 3 separators in the string, then they must be placed next to each other. "===".

Track 2 will be left unmasked if;

- The track2 data are *not* recognized to be in accordance with ISO/IEC 7813, or
- The track2 data are recognized to be in accordance with ISO/IEC 7813 and it is indicated as Private Label Card.

Track 2 will be masked as;

- PAN will be masked with 'A' according to PCI rules (6 + 4 digits unmasked). See Table 1-12.4,
- Service code will, if present, be masked with 'AAA',
- Expiration Date will, if present, be masked with 'AAAA',
- PIN Verification Data will, if present, be masked with 'AAAAA'.

Track 3

Track 3 will be left unmasked if;

- The track3 data is less than 8 characters
- The track3 data are recognized to be in accordance with ISO/IEC 7813 and it is indicated as Private Label Card.

Track 3 will be masked as;

- All characters will be masked with 'A',

ICC data

ICC data will be left unmasked if;

- Track2 Equivalent Data, Tag '57' and PAN Tag '5A' both indicate the card as a Private Label Card.

ICC data, if present, will be masked in the following way;

- Tag '57', Track 2 Equivalent Data, PAN masked with 'A' according to PCI rules (6 + 4 digits unmasked), see Table 1-12.4. Expiry Date, Service code and PVKI/PVV all masked with 'A'.
- Tag '5A' PAN masked with 'A' according to PCI rules (6 + 4 digits unmasked). See Table 1-12.4,
- Tag '5F 20' Cardholder Name masked with <space> except for "/",
- Tag '5F24', Application Expiry Date masked with 'AAAAAA',
- Tag '5F30', Service Code masked with '0AAA',
- Tag '5F34' Pan Sequence Number masked with 'AA',
- Tag '9F0B' Cardholder Name Extended masked with <space> except for "/",
- Tag '9F1F' Track 1 Discretionary Data masked with first 5 bytes with "A",
- Tag '9F20' Track 2 Discretionary Data masked with first 5 bytes with 'A'.

Example

A set of card data will be masked as shown below;

Table 1-10.12 - Examples of masking of PCI related data elements

Tag	Name	Base	Plain text	Masked text
'5A'	Application PAN	Hex	1234567890123456	123456AAAAAA3456
'5F20'	Cardholder Name	ASCII	DOE/JOHN	□□□/□□□□
'5F24'	Application Expiration Date	Hex	130127	AAAAAA
'5F30'	Service Code	Hex	0103	0AAA
'5F34'	Application PAN Seq. Num.	Hex	01	AA
'9F0B'	Cardholder Name Extended	ASCII	DOE/JOHN	□□□/□□□□
'9F1F'	Track 1 Discretionary Data	ASCII	14367834562199	AAAAA834562199
'9F20'	Track 2 Discretionary Data	Hex	14367834562199	AAAAA834562199

Legend: The character □ designates an ASCII <space>, i.e. '20'.

1-10.10.6 Dual Card Reference

The *Retrieve Card Data* command may return a Dual Card Reference as part of the response data. This makes it possible to use this command to retrieve a card reference without starting a transaction.

The Dual Card Reference obtained by use of the *Retrieve Card Data* command and the Dual Card Reference returned in the *Submit Card Reference 2* command is identical for the same card.

Retrieve Card Data (MSC)

A Dual Card Reference is always returned as part of the response, independently of whether the card is a Private Label card or not.

Retrieve Card Data (EMV)

If tag 'D4' is part of the Tag List given in the *Retrieve Card Data* command, a Dual Card Reference will always be part of the response, independently of whether the card is a Private Label card or not.

1-10.11 Token transactions

1-10.11.1 Introduction

Token based transactions are implemented in order to allow payment situations where the transaction amount is *not* known when the transaction is initialized.

A Token is used to temporarily store transaction data in a secure manner when a transaction cannot be completed immediately.

Example

As an example, a cardholder checks in at a hotel and expects to stay there for one week. An authorization is performed with an *estimated amount* for the entire stay. This will reserve the amount on the cardholders account.

After two nights the cardholder goes to the reception and wants to extend the stay for another week. A supplementing authorization is performed using an *additional estimated amount* to increase the amount authorized. The additional amount is reserved on the cardholders account as well.

When the cardholder checks out, the information related to the previous authorization is used to perform a transaction when the *exact amount* is known. The amount is now charged on the cardholders account, and the reservations are removed.

1-10.11.2 General requirements

1-10.11.2.1 A A Token shall only be used for a single transaction. For example, a Token used as input to a Supplementary Authorization shall not be used as input to a Capture transaction.

1-10.11.2.2 A A Token shall only be utilized in terminals belonging to the same chain of shops as the terminal creating the Token. The Merchant Number returned in the response to the *Initiate Token Based Payment* command can be used to identify the shop.

NOTE: The Merchant Number is also available from the Info field of the Token.

1-10.11.2.3 A A Token shall only be utilized in a terminal belonging to the same terminal environment as the terminal creating the Token. Therefore, position 1 and 2 of the POS Entry Mode shall be identical. See table 2-13.93 on page 2-13-72 for further details.

1-10.11.2.4 B The maximum number of outstanding Tokens handled by the Merchant Application shall match the actual environment.

NOTE: Example: At a gas station, the Merchant Application shall at least be able to handle as many Tokens at a time as the number of petrol pumps serviced.

- 1-10.11.2.5 A Cashback shall not be allowed for Token based transactions.
- 1-10.11.2.6 A It shall not be possible to utilize Merchant Initiative in a transaction that is based on an existing Token.
- When performing a Reversal (Authorization), no amount can be indicated.
- The retrieval of the Token from the Merchant Application is business dependent. For example, for payment of a rental car, the Token may be linked to the reference number of the rental contract.
- 1-10.11.2.7 A The terminal shall manage the maintenance of Tokens stored at the Merchant Application. When a Capture has been performed, the Token used as input shall, except for terminals supporting Post Registration, be deleted.
- 1-10.11.2.8 A Likewise, when a new Token has been created due to a Supplementary Authorization, the old Token shall be deleted.

Storage of the Token

- 1-10.11.2.9 A The MAD-Handler shall convey the Token to the Merchant Application by utilizing a *Write Handler String* command to Merchant Application Handler in case of an Original/Extended/Supplementary Authorization transaction.

1-10.11.3 Flow of information

This section describes the flow of information for a Token transaction.

The Business Calls;

- Original Authorization,
- Extended Authorization
- Supplementary Authorization,
- Capture, and
- Reversal (Authorization)

are covered by this section.

Based on the above mentioned Business Calls, a number of Token Macro Functions are defined. These Token Macro Functions are then used as building blocks for Special Functions. The Special Functions may be specific to different environments.

Figure 1-10.9 below depict the general flow of information in token based transactions.

The flow will start by the merchant requesting an Original/Extended Authorization. The result of this, including information on account number and amount, is stored in the Token. The authorization will generate a reservation on the cardholders account but not deduct funds from the account.

The merchant can, if there is a need for additional funding, perform a Supplementary Authorization. After this transaction, an additional amount is reserved on the account and the total amount is stored in a new Token.

The merchant will, once the precise amount is known, perform a Capture based on the Token. The transaction from

the Capture is sent to the Data Store, and further on to the host. This will deduct the specified amount on the account.

The merchant can, if the transaction is to be cancelled, perform a Reversal of the Authorization. This will release the reservation from the cardholders account.

Related to the hotel example in section 1-10.11.1 above;

- The initial reservation initiating an Original/Extended Authorization. A Token is generated by the PSAM and stored in the back office computer in the hotel.
- The subsequent reservation initiating a Supplementary Authorization. The original Token is sent to the PSAM along with other transaction data and a new Token is then returned. This Token is stored in the hotel back office for later use.
- When the cardholder checks out, the corresponding Token is used to perform a Capture. The output from the Capture transaction is a Financial Advice which is stored in the Data Store for transmission to the acquirer.

See for figure 1-10.9 for a graphical description of the flow.

1-10.11.4 Token based Transaction Types

Table 1-10.13 shows the seven types of Token based transactions.

Table 1-10.13 - Transaction Request Vs. Transaction Data

Transaction Request	Transaction Data	
	Input	Output
Original Authorization	Card read ¹⁾ / Key entered	Token
Extended Authorization	Card read ¹⁾	Token
Supplementary Authorization	Token	Token
Capture	Token	Financial Advice
Reversal (Authorization)	Token	Reversal Advice
Post Purchase	Token	Financial Request/Financial Advice
Post Refund	Token	Financial Request/Financial Advice

Legend: ¹⁾ Card read covers both EMV & MSC.

NOTE: Extended Authorization extends the Original Authorization by returning a "Card Reference" as well. This reference identifies the card in a uniquely way.

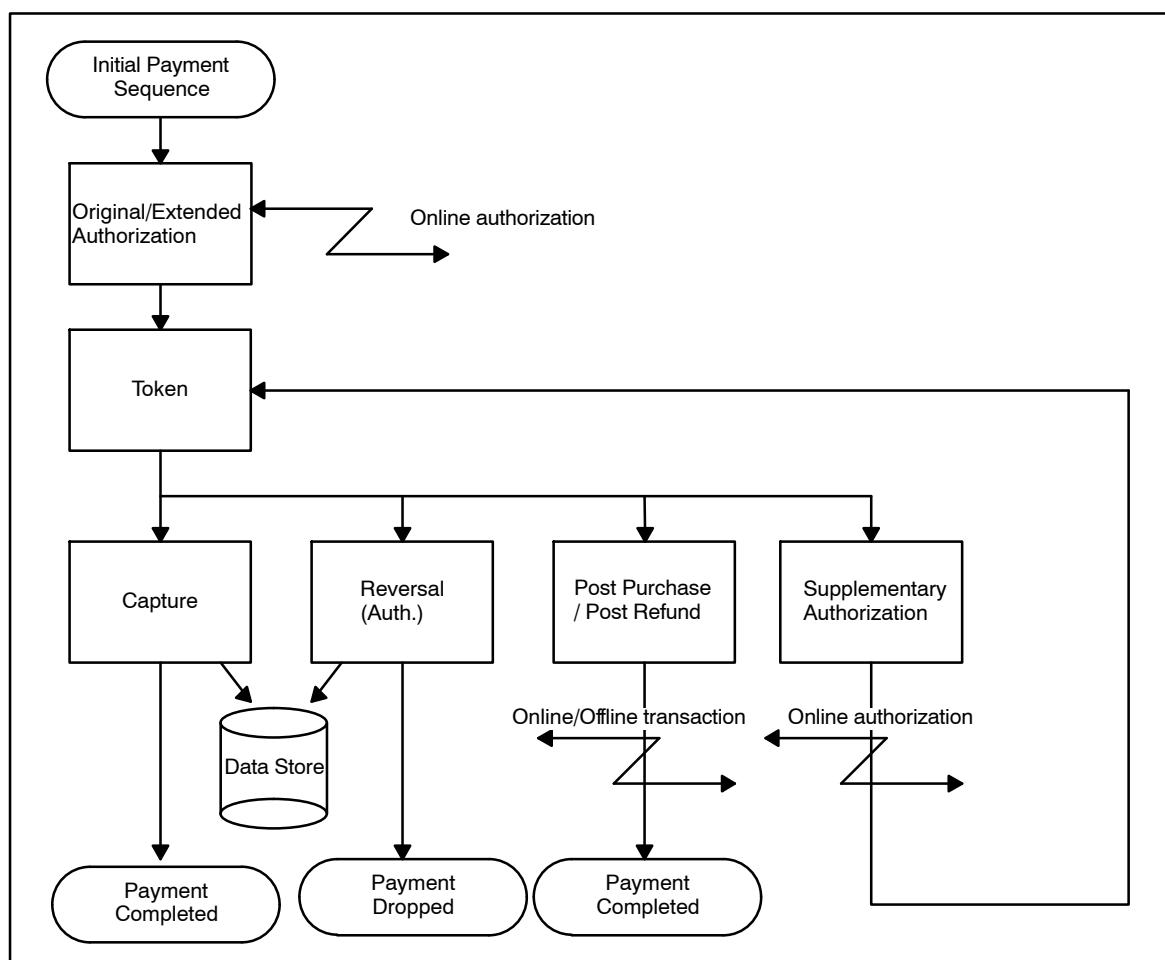


Figure 1-10.9 - Flow of Information - Token based Transactions

Token based transactions are intended to handle the following payment situations (examples):

- Fuel dispensers where an Original/Extended Authorization is performed before refueling may begin. A Capture will (automatically) be performed when refueling is finished and the exact amount is known.
- Ticket vending machines where an Original/Extended Authorization is performed before the ticket is generated. Once the ticket has been printed the Capture is (automatically) generated.
- Restaurants and similar environments where the cardholder chooses to pay an extra amount, typically gratuity. When the transaction is initiated, an Original/Extended Authorization is performed, after which the cardholder may add the gratuity. When this gratuity is known (or when the cardholder decides *not* to add any gratuity), then a Capture will be performed with the exact amount.
- Hotel and Car-rental, where the merchant initiates an Original/Extended Authorization during the check-in or the start of the lease. If it is recognized, during the stay or lease, that actual cost will overrun the original amount authorized, then one (or several) Supplementary Authorizations may be performed. Each Supplementary Authorization completed successfully will augment the total amount authorized. When the final payment is to be performed, typically at check-out or

when ending the lease, a Capture with the exact amount will be performed.

- Independently of the payment situation (but typically for fuel dispensers and hotels), it may happen that an authorization is not utilized subsequently. The cardholder did not start to fill up the tank with petrol during the assigned time slot at an Automated Fuel Dispenser, or the cardholder decides to pay with another card during check-out at a hotel. In a situation like this a Reversal (Authorization) is initiated in order to release the amount reserved on the cardholders account.
- The Business Calls Post Purchase and Post Refund are typically used *after* a Capture has been performed, if either unexpected expenses arise later or funds are to be returned due to lesser expenses than expected.

1-10.11.5 Token - Contents and Identification Keys

The basic information of a Token is defined in table 1-10.14 and figure 1-10.10 below, but a Token may as well contain certain business specific information.

When a Token is handed over from the PSAM to the terminal (and possible further on to the cash register system), only the basic information defined in the figure 1-10.10 is included.

Similar, when a Token is transferred to the PSAM, only the basic information is to be conveyed.

The basic information may not be sufficient, when a Token is stored by the terminal. Further information may be needed to be able to find the Token again, even though a small part of the Token is in plaintext.

The additional data elements needed to identify a Token may depend on the actual business environment. Different data elements may be used as the key to find the Token again. From a general point of view, the following 4 types of data keys given in table 1-10.14 should cover the needs in all business environments (even though not all identification keys are relevant in all environments). It may as well be necessary to store some additional data in the token for some transactions.

Table 1-10.14 - Token Identification Key

Token Identification Key	Description
"Terminal Key"	<p>A unique key assigned by the terminal, when the initial Token is received from the PSAM.</p> <p>The unique Terminal Key may also be used to identify derived Tokens after Supplementary Authorizations has been performed.</p> <p>Example: The following data elements may form part of a Terminal Key:</p> <ul style="list-style-type: none"> • part of the PSAM ID, e.g. the last 6 digits, • the STAN (6 digits) • one or more check digits or a random number.
"Card Reference Key"	<p>A key derived from the PAN of the actual card in use. Other data elements, e.g. the PAN Sequence Number may also form part of the computation.</p> <p>The Card Reference Key shall not disclose the PAN or part of the PAN.</p> <p>Example: The result (or part of the result) from a secure hash computation may be used as Card Reference Key.</p> <p>The "Card Reference" from the "Extended Authorization" business call is such a key.</p>
"Text Key"	<p>In some business environments it may be relevant to attach a specific business information.</p> <p>Examples: The room number may be a relevant key in the hotel environment, and for car rental the number on the agreement may be relevant.</p> <p>To be able to support different formats, a 'free field' Text Key should be available.</p>
"Token Date"	<p>The Token Date is not a key like the three other keys. The Token Date should be used to control and verify the life of the Token.</p> <p>The Token Date should indicate the date when the initial Token was generated.</p>
<p>NOTE: The number of bytes assigned for each key may depend on the level of uniqueness given for the different keys.</p>	

When a Token is stored in the Merchant Interface part of the payment system, including search and identification keys, the total block of data may look like this:

Terminal Key	Business specific information and Token identification keys
Card Reference Key	
Text Key	
Token Date	
(additional data elements)	
Token INFO (plaintext)	Basic Token information exchange to and from the PSAMs
Token Data (enciphered)	

Figure 1-10.10 - Token - Merchant Interface

The number of business specific data elements shown on the figure above shall only be seen as guidelines, since implementation in specific environments may require that further information shall be assigned to the Token.

Examples: The following list shows a number of additional data elements, which may be relevant and attached, when a Token is stored:

- In case of a DCC transaction: The amount authorized indicated in the merchants local currency may be relevant. The amount indicated in the cardholders billing currency appears in the Token INFO field.
- If surcharge is relevant, information about calculation formula used may be needed in later steps of the transaction sequence.
- For certain regional solutions, information on Account Type selection, and Payment Condition Code may be relevant.
- In case of a transaction with Account Type Selection performed, the account type selected. This is not stored in the Token INFO field.
- For certain regional solutions Acquirer Information to be used during Capture, as this information is not stored in the Token INFO field.
- Information from the Extended Issuer Envelope generated during the Authorization and needed during the Capture, see section 1-10.5.2. This information is not stored in the Token INFO field.

1-10.11.6 Token and Cardholder verification method

The "Cardholder Verification Method" (CVM) to be used for the particular transaction (e.g. PIN, Signature or No CVM) is determined when performing the Original/Extended Authorization.

- 1-10.11.6.1 A If PIN is selected, the PIN shall be entered and be verified when performing the Original/Extended Authorization (e.g. for a fuel dispenser).

- 1-10.11.6.2 A As the exact amount is not known when performing the Original/Extended Authorization, PIN entry shall not be combined with confirmation of the amount as for a “normal” Purchase.
- 1-10.11.6.3 A If signature is selected, the cardholder shall not sign the receipt until the Capture, where the exact amount is present (e.g. during check-out in a hotel).
- NOTE:** The signature may be available as a “Signature on File” to allow for express checkout.
- If the total amount authorized exceeds the exact transaction amount defined in the Capture, a partial reversal may automatically be initiated by the host, in order to “release” the difference.
- 1-10.11.6.4 A The terminal (PSAM) shall not initiate Partial Reversals.
- 1-10.11.6.5 C Authorizations and Captures may be geographically, PSAM and/or time separated.

1-10.11.7 Token Management Functions

General Requirements

- 1-10.11.7.1 A Each time a Token is forwarded from the PSAM to the terminal, the terminal shall ensure that the Token is stored satisfactorily.
- 1-10.11.7.2 A When the PSAM requests a Token, the terminal shall be able to retrieve the Token.
- 1-10.11.7.3 C The terminal may also be able to verify that a Token coming from the “Token Store” is the ‘correct’ Token to be used in the present transaction.
- To be able to handle the Tokens correctly a number of different functions are needed by the terminal. A basic set of functions is described below. The description is based on the assumption that all 4 identification keys from table 1-10.14 are used, as explained in the table.

Save Token

- 1-10.11.7.4 A Each time a Token based payment sequence is initiated the original Token shall be stored temporary for later use.
- 1-10.11.7.5 A The terminal shall be able to attach the additional data elements required for identification of the Token.
- 1-10.11.7.6 A If the amount authorized has been increased by performing a Supplementary Authorization, the original Token shall be replaced by the new Token received from the PSAM. The terminal shall be able to maintain the identification data attached to the Token.

Find Token

- 1-10.11.7.7 A When a previously stored Token shall be retrieved again, the terminal shall be able to obtain the relevant identification data.
- NOTE:** The “Card Reference” from the Business Call “Extended Authorization” could be used to identify transactions performed with the same card.

1-10.11.7.8 A Only one Token should match the search key used, but if more than one match is identified, the terminal shall be able to handle this condition as well.

1-10.11.7.9 C When a Token is retrieved, the Token may be too old. The terminal should validate the Token Date and reject the Token if the time-limit has expired. A reversal of the token shall be generated if the time limit of the token has expired. Alternatively, the terminal should notice the operator, and let him/her decide the next step.

NOTE: The actual time-limit for the validity of the authorization obtained is dependent on e.g. the card product used to obtain the authorization and the business segment for which the business is registered.

Verify Token

1-10.11.7.10 C If one of the identification keys is used to find the Token, another key may be used to verify that the Token found corresponds to the actual business situation and the actual customer card.

Example:

A hotel uses the Text Key as the primary key to identify and find Tokens. The Text Key contains the room number.

When the cardholder checks out from the hotel, the Token is found before the final Capture is initiated. The search for the Token is based on the room number.

To be sure that the Token is built upon the actual customers card data, the card may be read again, and the Card Reference may be computed again.

If the Card Reference stored together with the Token is identical to the value computed from the card, there should be no risk of mix up between the Tokens.

Search for specific Tokens

If Tokens have been saved, but never retrieved again, the storage may after a period contain a number of expired and unusable Tokens.

1-10.11.7.11 A To be able to identify such unusable Tokens, the terminal shall include a function to setup relevant search criteria. When Tokens are retrieved, and it has been verified that they are no longer valid, these Tokens shall be deleted from the storage. A reversal for these tokens shall be generated as well.

1-10.12 Token Macro Functions

Some business environments have specific requirements concerning the functions supported.

To be able to support such different requirements, a number of different Business Calls are defined and supported by the PSAM.

Based on the Business Calls and the business requirements concerning specific functions, a number of general Token Macro Functions have been defined.

This section defines and describes the most common Token Macro Functions. These Token Macro Functions should make it possible to cover most business requirements.

The names of the Token Macro Functions have been selected to avoid duplicates of the Business Call's. The names are:

- MAKE PURCHASE
- AUTHORIZE
- AUTHORIZATION ADD
- FINALIZE
- RELEASE
- MAKE REFUND
- AUTHORIZE WITH TIPS
- FINALIZE WITH TIPS

Depending on the actual business environments, other names may be more descriptive. The Token Macro Functions include the handling of DCC in the flow.

1-10.12.1 Macro MAKE PURCHASE

The macro MAKE PURCHASE is used if the exact amount to pay for goods and services are known, when the payment sequence is initiated.

Tips/gratuity may be added if relevant.

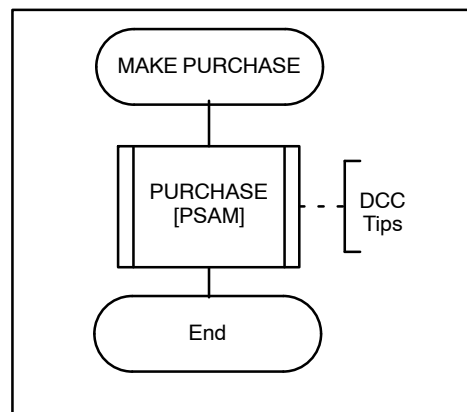


Figure 1-10.11 - The Macro MAKE PURCHASE

1-10.12.2 Macro AUTHORIZE

The Macro AUTHORIZE is used if the exact amount to pay for goods and services is not known when the payment card is presented to the merchant, i.e. at check-in at a hotel.

If an Authorization (Token) already exists, this previous Authorization (Token) may be replaced or just used instead.

- 1-10.12.2.1 A If validation of the card is the only purpose of the AUTHORIZE macro, the amount used shall be configurable.

- 1-10.12.2.2 C If validation of the card is the only purpose of the AUTHORIZE macro, the same amount value may be used for all card schemes.
- NOTE:** The amount value depends on the merchant category. A value of 1,00 or the maximum amount are used for authorization at Automated Fuel dispensers. See ref. 38: "MasterCard, Europe Region Operations Bulletin No. 1"
- 1-10.12.2.3 A If DCC is an option for the actual card, the decision about the Cardholder currency to use shall be taken during AUTHORIZE.

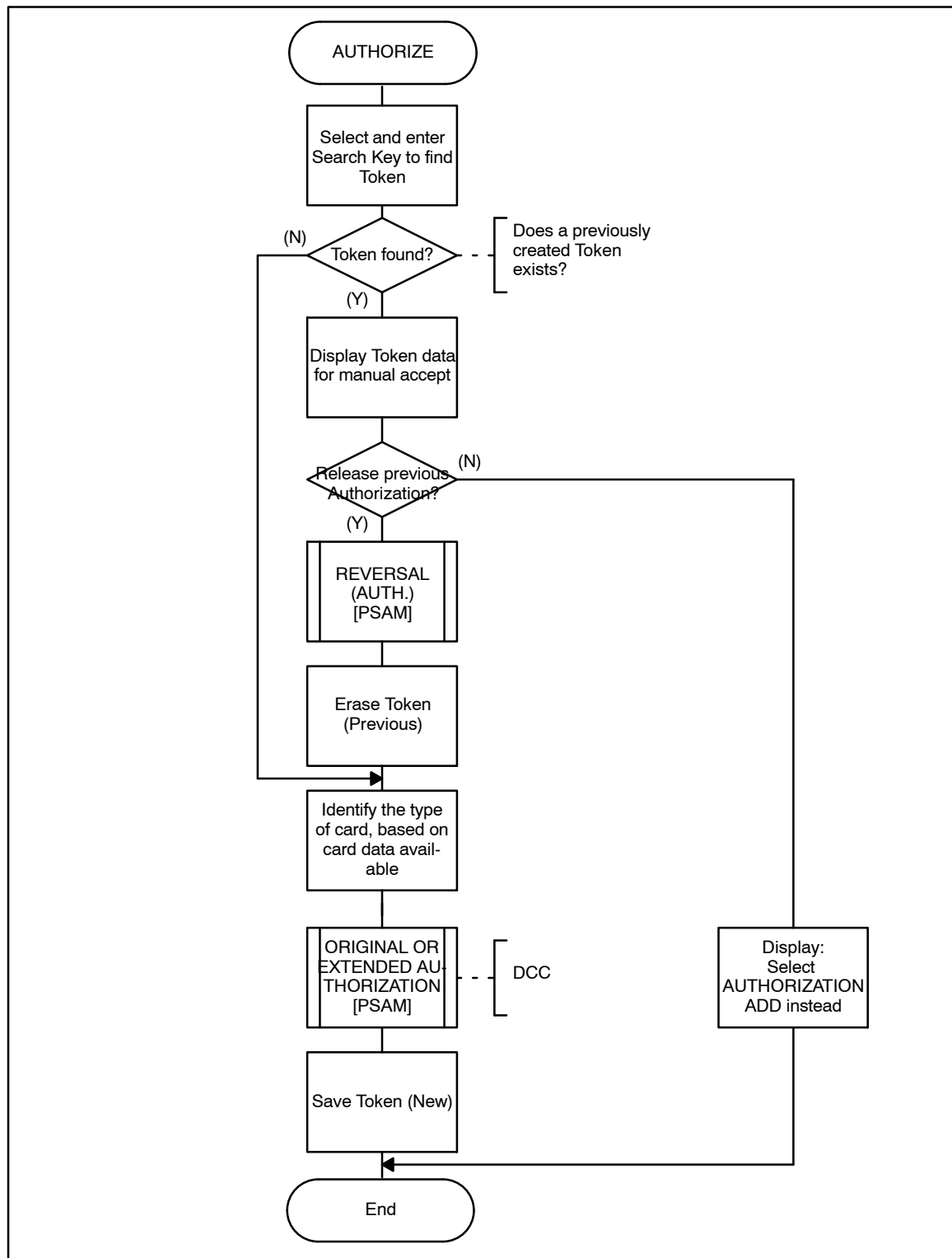


Figure 1-10.12 - Macro AUTHORIZE

1-10.12.3 Macro AUTHORIZATION ADD

The macro AUTHORIZATION ADD is used when an Authorization has been completed previously, but the amount authorized shall be increased. The card is not used when performing this macro.

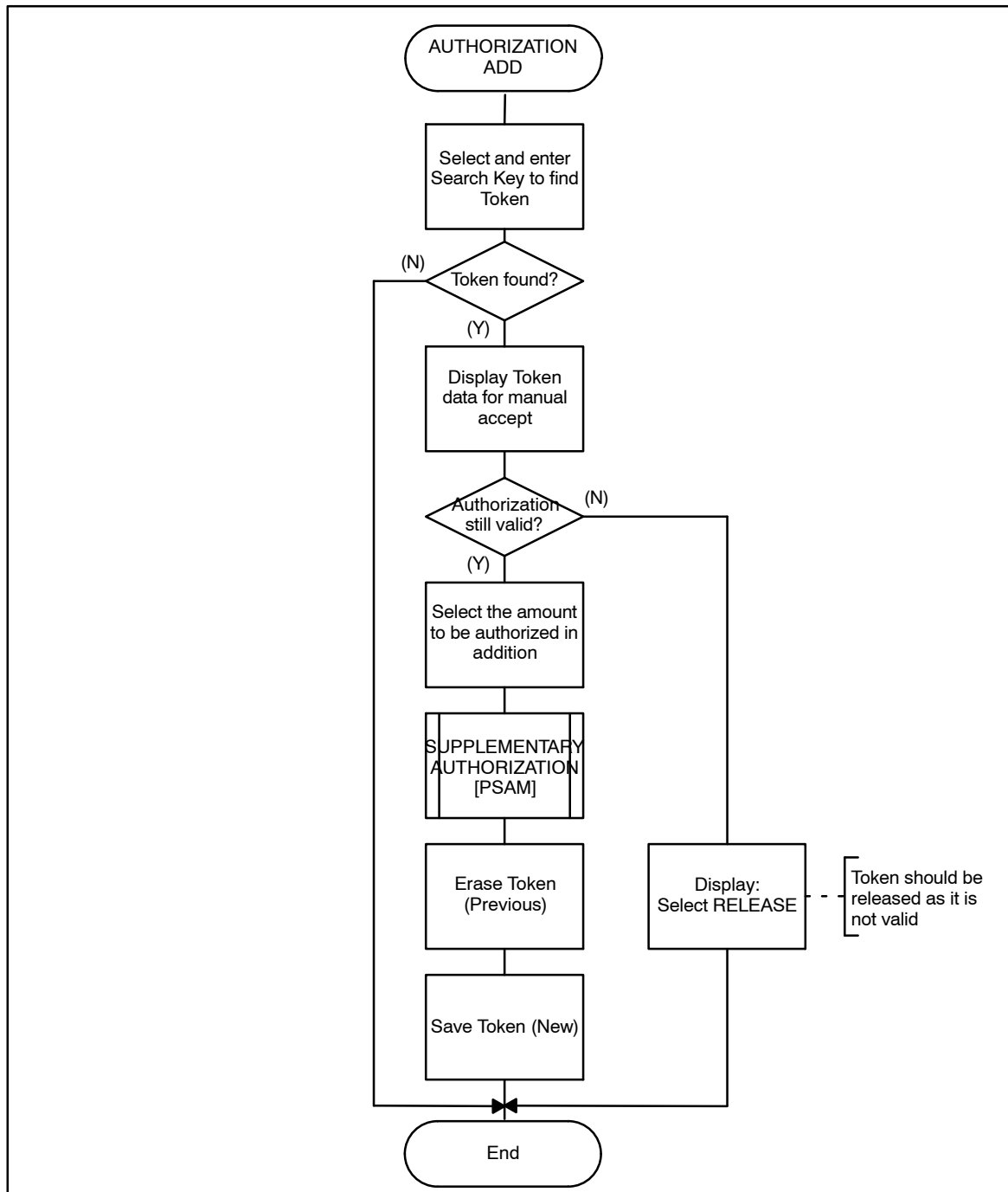


Figure 1-10.13 - Macro AUTHORIZATION ADD

1-10.12.4 Macro FINALIZE

The macro FINALIZE is used when the exact amount to pay for goods and services is known, after an AUTHORIZE and maybe one or more AUTHORIZATION ADDs has previously been performed.

Tips/gratuuity may be added if relevant.

- 1-10.12.4.1 A Irrespective of the cardholder verification method used during the previous Token Macro Functions, a receipt for the cardholders signature shall be printed. The cardholder always accepts the final amount including any surcharge and tips/gratuity by signing the final receipt.
- NOTE:** The cardholder signature may be available as a "Signature on file".
- 1-10.12.4.2 A If DCC has been selected during the initial Authorization, a pre-receipt showing the amount to pay in the cardholder's billing currency shall be printed. This receipt may also include a field for adding tips/gratuity.
- 1-10.12.4.3 A If DCC has been selected previously, but the cardholder reconsider and decides not to complete the payment in his/her billing currency, a RELEASE shall be initiated instead, followed by a Purchase in the merchant local currency.
- The flow of FINALIZE is shown in figure 1-10.14, but this figure does not include the handling of DCC.
- Decision to be taken during transactions concerning e.g. whether a Token is still valid or an amount is sufficient may be taken automatically by the terminal or manually by merchant.
- 1-10.12.4.4 A If the decision is taken automatically, the size of the deviation accepted shall be configurable.
- NOTE:** The general rule is that the amount captured may exceed the amount authorized with up to 15% without initiating an additional authorization. But this rule may be overruled by merchant specific acquirer agreements.

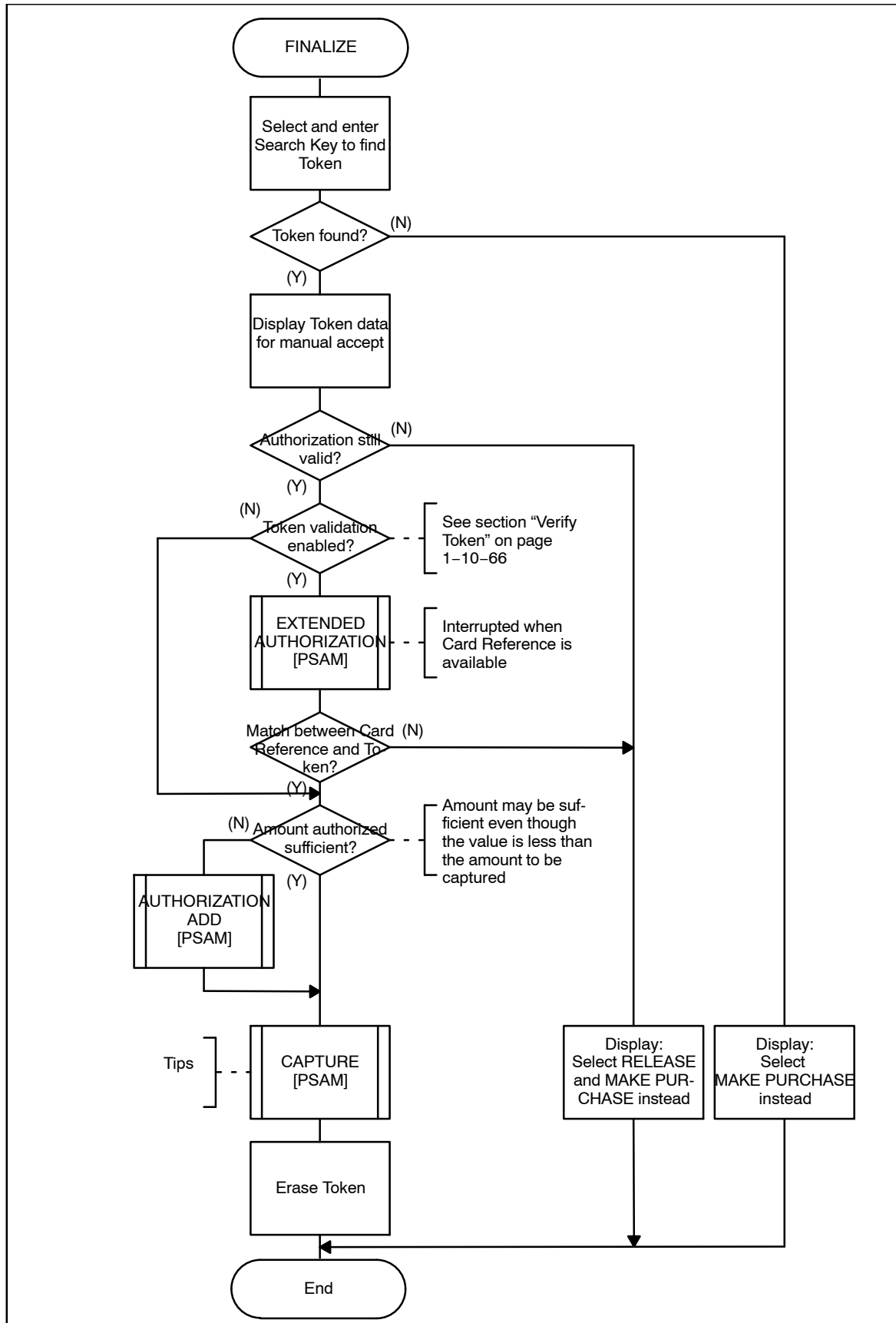


Figure 1-10.14 - Macro FINALIZE

1-10.12.5 Macro RELEASE

The macro RELEASE is used when an Authorization and maybe one or more Additional Authorizations have been performed, but the FINALIZE is not going to be performed.

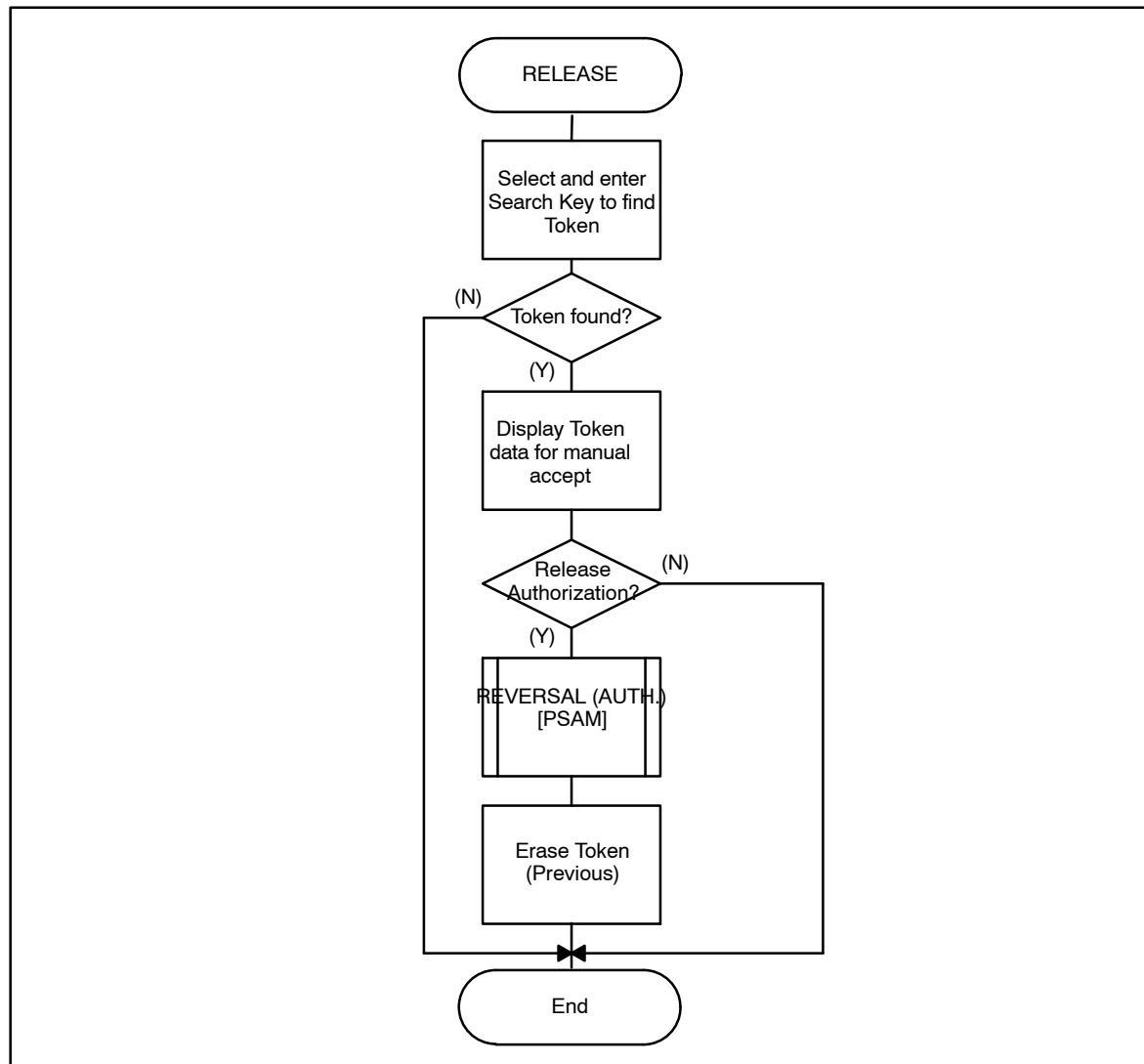


Figure 1-10.15 - Macro RELEASE

1-10.12.6 Macro MAKE REFUND

The macro MAKE REFUND is used when the cardholder returns any goods, and the cardholder is going to be credited the original transaction amount - either completely or partly.

If tips/gratuity formed a part of the original transaction, tips/gratuity may also be specified in the Refund.

The flow of the macro MAKE REFUND is shown below.

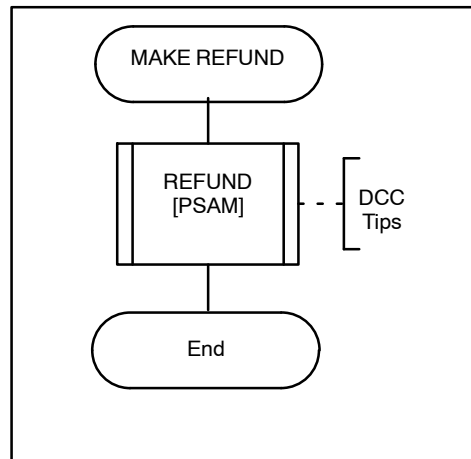


Figure 1-10.16 - Macro MAKE REFUND

1-10.12.7 Macro AUTHORIZE FOR TIPS

This macro is intended to be used in environments where tips is an option and signature is the preferred cardholder verification method.

The flow diagram shown in figure 1-10.17 and the following description explains the flow during this Token Macro Function.

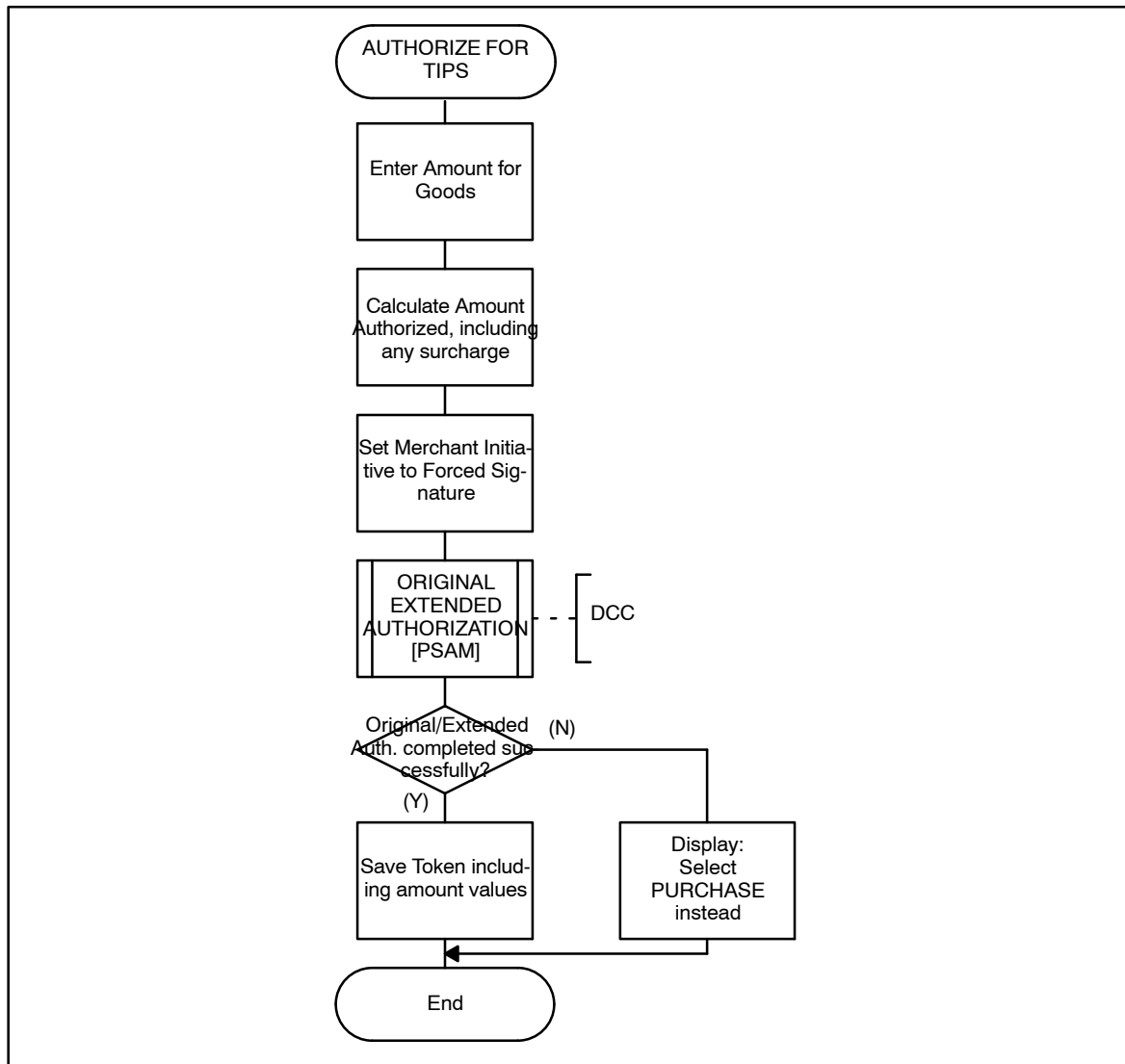


Figure 1-10.17 - Macro AUTHORIZE FOR TIPS

Description:

1. The amount to pay for goods and services is entered and the card is swiped/inserted in the terminal.
2. Based on the amount and the actual card, the terminal computes the value for Surcharge (if any).
3. The standard Business Call ORIGINAL/EXTENDED AUTHORIZATION is initiated based on

$$\text{Amount} = \text{Amount to pay for Goods and Services} + \text{Surcharge.}$$

$$\text{Merchant Initiative} = \text{Forced Signature.}$$
4. If DCC is an option for the actual card, the cardholder may be offered the option of paying in the cardholders billing currency. The pre-receipt printed for the DCC decision may or may not include free space for addition of tips/gratuity. If space for tips/gratuity is included, the similar field shall be omitted on the transaction receipt signed by the cardholder.
5. If the ORIGINAL/EXTENDED AUTHORIZATION is NOT completed successfully, the transaction must be com-

pleted as a standard PURCHASE Business Call instead. The standard call of PURCHASE shall be initiated without any force-indicators. Therefore the corresponding PIN code may be required during the PURCHASE. Tips/gratuity is not an option during PURCHASE, unless the tips/gratuity amount is included in the amount authorized online.

6. If the ORIGINAL/EXTENDED AUTHORIZATION is completed successfully the Token received as output from the ORIGINAL/EXTENDED AUTHORIZATION shall be stored by the terminal together with the corresponding amount values (Amount to pay for goods and services and the Surcharge amount, if added). The data elements needed to print the receipt again, but with tips/gratuity included shall be stored together with the Token. The search keys needed to find the Token again shall also be included in the data package saved.
7. A corresponding pair of receipts (the merchants original and the cardholders copy) shall be printed. These receipts shall show the amount to pay for goods and services, and any surcharge added. The receipts may include free space for adding tips/gratuity and the cardholders signature.

1-10.12.8 Macro FINALIZE WITH TIPS

This macro shall be used to complete the payment sequence initiated by the macro AUTHORIZE FOR TIPS.

The flow diagram shown in figure 1-10.18 and the following description explains the flow during this Token Macro Function.

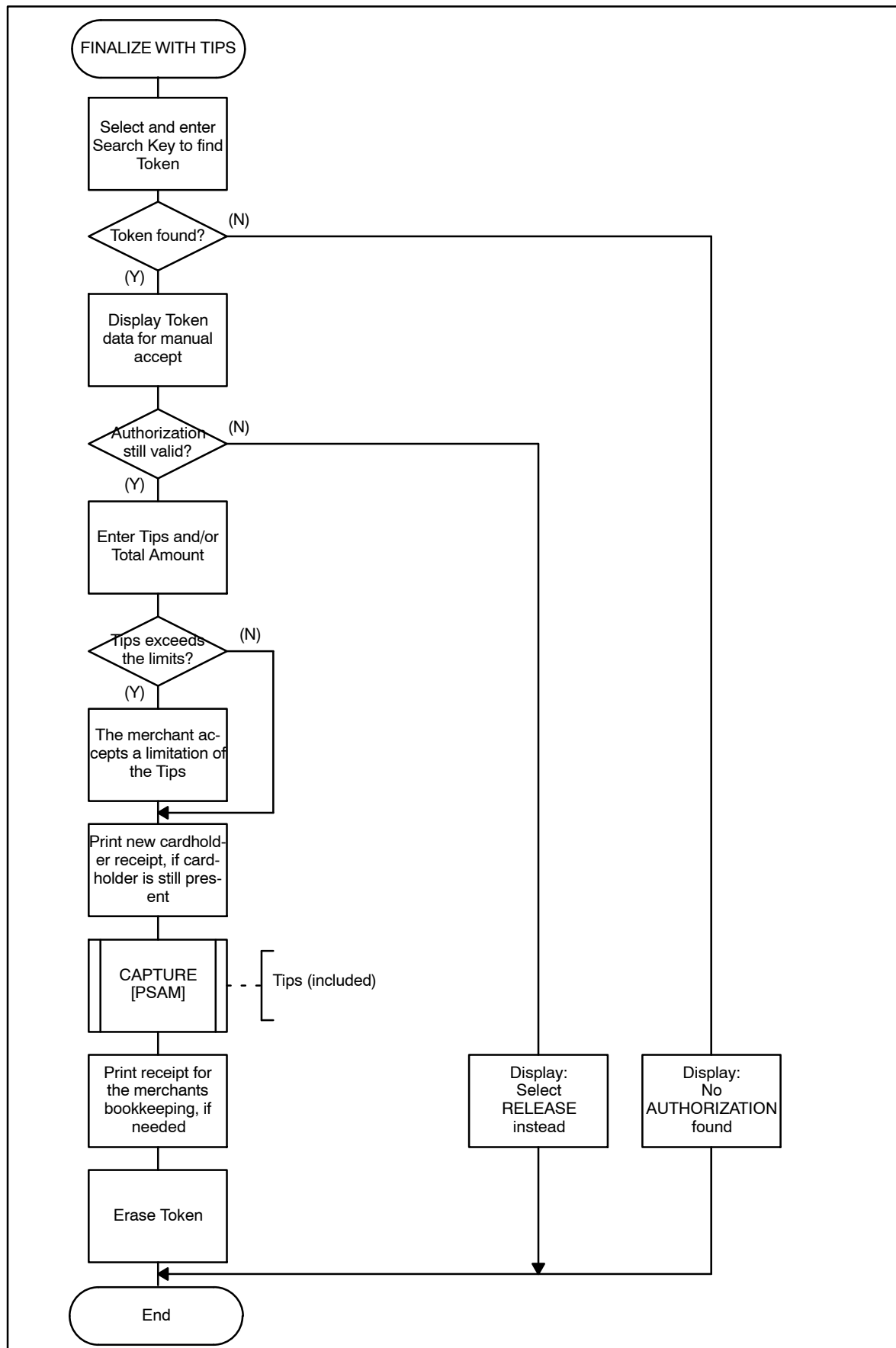


Figure 1-10.18 - Macro FINALIZE WITH TIPS

The sequence of the following requirements (1-10.12.8.1 - 1-10.12.8.11) describe the normal procedure for FINALIZE WITH TIPS:

NOTE: Debit cards may decline this type of transactions.

- 1-10.12.8.1 A When the cardholder has signed the receipt and added any tips/gratuity, the merchant shall immediately complete the payment sequence by initiating the Token Macro Function FINALIZE WITH TIPS.
- 1-10.12.8.2 A Based on the search key(s) used, the Token shall be found.
- 1-10.12.8.3 A If no Token is matching the search key(s) entered, the merchant shall be informed about the result.
- 1-10.12.8.4 A If a corresponding Token is found, the relevant transaction data shall be displayed to the merchant. The transaction data display shall enable the merchant to decide whether the correct Token is found or not, and whether the Token is still valid.
- 1-10.12.8.5 A If the merchant does not accept the Token found, the terminal shall suggest that the Token is released, using the Token Macro Function RELEASE.
- The merchant enters the tips/gratuity added by the cardholder and/or the new transaction amount.
- 1-10.12.8.6 A The merchant shall not be able to add an extra amount that exceeds the limits defined by local legislation (in Denmark 15% and 1000 DKK). If the tips/gratuity added by the cardholder cause that the total amount exceeds the limits, the merchant may instead accept the maximum value.
- 1-10.12.8.7 A If the cardholder is still present and waiting for a receipt including the tips/gratuity too, this receipt shall be printed.
- 1-10.12.8.8 A The additional receipt printed for the cardholder shall be based on the same data elements as the receipt signed by the cardholder. That means that the additional receipt shall also be based on the data elements received during the ORIGINAL/EXTENDED AUTHORIZATION.
- 1-10.12.8.9 A The standard Business Call CAPTURE is initiated. If the CAPTURE is initiated long time after the cardholder was present, the final transactions details, especially the date and time information, will be misleading. Therefore the Token Macro Function FINALIZE WITH TIPS and with that the CAPTURE shall be initiated in continuation of the cardholder signing the receipt.
- 1-10.12.8.10 C If the merchant needs transaction documentation, the merchant may print a receipt based on the data element from the CAPTURE. This receipt is for internal use by the merchant and shall not be handed over to the cardholder.
- 1-10.12.8.11 A The Token used to complete the CAPTURE shall be destroyed.

1-10.13 Special Functions

1-10.13.1 Special Functions - Hotels

In the hotel environment a number of specific functions are required. The main functions are listed and explained in this section.

The short description of each Merchant Function also includes a reference to the Token Macro Functions behind and how to use these functions. The Macro Functions are shown capitalized, as in their definition, like AUTHORIZE.

Card Validation (Booking)

- 1-10.13.1.1 C When a booking or reservation is initiated, the hotel may validate the authenticity of the card data received from the customer.
- 1-10.13.1.2 A To validate the card data received, the hotel shall perform an AUTHORIZE with an amount of 1 major unit of the local currency (like 1,00 DKK). The card data is key entered.
- NOTE:** The value for the terminal is specified as a single currency unit. The requirements may vary for the different card schemes. This is handled by the Host.
- 1-10.13.1.3 A The result of the AUTHORIZE (i.e. the Token received from the PSAM) shall not be stored. How to skip the storage may depend on the actual implementation.

Guaranteed Reservation

Before the customer arrives, the hotel may want to be sure that they get paid.

- 1-10.13.1.4 A To obtain a guarantee the hotel shall perform an AUTHORIZE with an estimated amount. The card data is key entered. The Token shall be stored.

The Authorization may later on be used as guarantee for a 'no show payment'.

The Authorization may also be used as first step in the payment sequence, in situations where the card used does not belong to the hotel guest, i.e. the reservation and the payment is done by another person/company not present.

Check-In - Card present

When the hotel guest arrives, he/she will normally bring the card to be used for the payment.

Based on the physical card available the hotel performs an AUTHORIZE.

- 1-10.13.1.5 A If any Authorization has been completed before the guest arrives, this Authorization shall be released, either automatically as part of the AUTHORIZE flow or by selecting RELEASE.

Check-In - Card not present

If the card used for the payment is not present when the guest arrives, only key entering is possible.

- 1-10.13.1.6 B The hotel shall perform an AUTHORIZE based on the key entered card data if the card is not present.
- 1-10.13.1.7 C If any Authorization has been completed before the guest arrives, this Authorization may still be valid. The sales assistant should be guided to perform an ADD AUTHORIZATION instead, if the Authorization is still valid, but the amount shall be increased.
- 1-10.13.1.8 A If an invalid Authorization already exists, this Authorization shall be released, either automatically as part of the AUTHORIZE flow or by selecting RELEASE.

Additional Authorization

- 1-10.13.1.9 A If the guest's consumption exceeds the estimated amount, and the hotel wants to increase the amount authorized, an ADD AUTHORIZATION shall be performed.

If the existing Authorization is no longer valid, the sales assistant shall be guided to release the Authorization by performing a RELEASE. The Guest should be called to the reception desk, and a new AUTHORIZE should be performed.

Cancel Authorization

- 1-10.13.1.10 A If an Authorization has been completed, but it appears that other means of payment is going to be used, the hotel shall release the Authorization by performing a RELEASE.

Check-Out - Cardholder present

The FINALIZE function is used during check-out, if any Authorization is available.

- 1-10.13.1.11 B If a valid Authorization is available, this Authorization shall be used as input during FINALIZE.
- 1-10.13.1.12 A If an invalid Authorization is available, the sales assistant shall instead be guided to perform a RELEASE followed by a MAKE PURCHASE.
- 1-10.13.1.13 C If the amount covered by the Authorization is not sufficient compared to the invoice amount, an ADD AUTHORIZATION may automatically or manually be initiated as part of the FINALIZE function.

NOTE: The amount authorized may be sufficient even though the final amount is slightly higher. The rules may depend on the individual card schemes.

- 1-10.13.1.14 C If no Authorization is available, the sales assistant should be guided to perform a MAKE PURCHASE.

Alternatively a MAKE REFUND may be needed if a deposit has been paid, and the deposit amount exceeds the invoice amount.

Check-Out - Cardholder not present

There may be different reasons why the cardholder is not present at the time of Check-Out.

The guest has never arrived ('no show'), the card used does not belong to the guest or the guest has already left the hotel ('express check-out').

The functions to follow are the same as if the cardholder was present - as explained above and irrespective of the reason why the cardholder is not present.

1-10.13.2 Merchant Functions - Restaurant

When the payment sequence is initiated in the restaurant environment, the amount to pay will be known. The bill handed over to the cardholder shows the total amount.

Only surcharge (depending on the means of payment) and tips/gratuities may still be unknown.

Therefore the only Token Macro Function to be used in the restaurant environment is MAKE PURCHASE (except if a Refund is needed to credit a previous payment).

If the cardholder is not able to be face-to-face with the terminal during transaction processing, the Token Macro Function AUTHORIZE FOR TIPS may be an alternative if accepted by the acquirers.

1-10.13.3 Merchant Functions - Car Rental

When a cardholder makes a reservation for a car, the procedure is similar to the procedure used, when a reservation for a hotel room is received.

When the car is collected, the procedure is similar to the procedure used, when a guest checks in at a hotel.

When the car is returned, the procedure is similar to the procedure used, when a hotel guest checks out.

Therefore, the description of Merchant Functions for the hotel environment is expected to cover the car rental business too.

1-10.13.4 Token and Unattended Payment Terminals

There is in certain business environments a need of relating a previous authorization or transaction to a specific PAN, without revealing information about the PAN. This can be achieved by using the Card Reference from the Business Call Extended Authorization.

The following scenarios are foreseen;

For an Automated Fuel Dispenser, it should be possible for the cardholder to get only the correct receipt, after the transaction is over. This could be achieved in the following way;

The (original) transaction is initiated using the Extended Authorization and the cardholder is asked if a receipt is re-

requested. The Card Reference is stored together with the receipt information. The terminal will, when the card is inserted (again after the transaction) start an Extended Authorization again. It will compare the Card Reference generated with the values stored together with the receipts. If a match is found, it will print the corresponding receipt, and terminate the transaction. If no match is found, the transaction continues.

For a Parking solution, it should be possible to link the information retrieved when the parking area is entered, with the card used, when leaving the parking area. This could be achieved in the following way;

A transaction using the Extended Authorization is initiated when the parking area is entered. The Card Reference is stored together with the information on entry time and so on. The terminal will, when the card is inserted at exit start an Extended Authorization. It will compare the Card Reference generated with the values stored together with the entry information. If a match is found, it retrieves the entry information, terminates the transaction, calculates the fee and perform the financial transaction.

1-10.14 DCC - Dynamic Currency Conversion

1-10.14.1 Introduction

The basic element for DCC is the possibility of offering the cardholder to carry out a card transaction in the cardholders billing currency, instead of the merchants local currency.

If a terminal offers DCC, it is the cardholders choice to decide whether DCC shall be accepted or not.

Even though a DCC transaction is completed in the cardholders billing currency, the merchant is settled in his local currency.

To be able to convey transaction amounts in two currencies, the implementation of DCC imply a number of additional data elements to be included in a DCC transaction.

In this section, the name DCC-Transaction-Information is used for the additional DCC information to be transferred.

This section defines the technical requirements for implementing the DCC-Transaction-Information in attended terminals.

Conditions for DCC

The international card schemes have specified the rules for the DCC functions. The requirements defined by MasterCard, Visa or other card schemes for terminals supporting DCC are not listed in this document.

The use of DCC for UPT's are under consideration.

When DCC is implemented, a table of relevant prefix ranges and corresponding currency codes and exchange rates must

- be available to the terminal. The table should also include information of the period in which it is applicable.
- 1-10.14.1.1 A The terminal shall ensure that DCC is not offered if the if the table is outdated.
- How this currency table is made available to terminals and how this table is validated , is outside the scope of this document.
- Agreements between the merchant and the acquirer concerning the use of DCC terminals are outside the scope of this document.
- NOTE:** The setup of the DCC tables should ensure that DCC is not offered for national cards.
- 1-10.14.1.2 A The selection of procedures for Dynamic Currency Conversion (i.e. cardholder decision of paying in his/her billing currency instead of the merchants local currency) shall only be an option for the following Business Calls:
- Purchase,
 - Original/Extended Authorization and
 - Refund
- The decision about the transaction currency to be used is taken when the transaction sequence is initiated. A dialogue with the cardholder is possible when the card is presented to the sales assistant.
- The actual selection may be performed either by the merchant based on the response from the cardholder or by the cardholder based on information presented on the terminal.
- NOTE:** The information to the cardholder may either be available in a pre-receipt, or on the terminal display combined with a leaflet.
- 1-10.14.1.3 A Since the PAN controls whether DCC is an option or not, the DCC decision shall be taken after the card has been inserted/swiped in the terminal and before the cardholder accepts any amounts.
- 1-10.14.1.4 A If DCC is selected for a Token based transaction sequence, the currency selected during the Original/Extended Authorization shall be the currency to be used through the complete sequence, including the Capture. If the cardholder changes his mind at a later stage, then the current transaction has to be cancelled, and a new initiated.
- The exchange rate to be used is the exchange rate valid at the time when the transaction is performed. That is, the exchange rate may change from an Original/Extended Authorization is initiated and until the corresponding Capture is completed.
- The cardholders decision about the currency to be used is either to be based on a printed pre-receipt showing the amount to pay (or the estimated amount in case of a Token based sequence) or on a cardholder performed selection dialogue. The cardholder performed selection dialogue is based on a preprinted information on a flyer or on the terminal and dynamic information displayed on the terminal.
- 1-10.14.1.5 A A pre-receipt shall show the amount in both the merchants local currency and the cardholders billing currency, together with information about the exchange rate.

- 1-10.14.1.6 A It shall not be possible to combine DCC and cashback.

NOTE: This is a card scheme requirement.

1-10.14.2 Getting the DCC pre-information

The BIN is used by the terminal to determine whether or not DCC can be performed, and the currency to offer.

The figures below (1-10.19 - 1-10.22) shows how retrieving the DCC pre-information may fit into the general transaction flow.

Two flows are necessary to describe the handling of EMV and MSC cards. The first figure, 1-10.19, describes the handling if a MSC is used or if an EMV card is used and no preliminary information about the amount is requested by the card. The second figure, 1-10.20, describes the handling if an EMV card *requires* amount related information to be present early in the card payment sequence - i.e. before the BIN is known to the terminal.

NOTE: This latter flow will generate an additional (prematurely terminated) transaction.

As the selection is to be completed before any PIN entry is initiated, the transaction flow for magnetic stripe transactions (MSC) may differ somewhat from the flow for EMV cards (ICC), but seen from the cardholders as well as the merchants point of view, there will be no difference.

Requirements for Card Data Protection makes track 2 data unavailable outside a secure environment, unless the BIN-range has been specifically marked as allowed to be published.

- 1-10.14.2.1 B When an MSC transaction is initiated, the terminal shall issue an *Initiate Payment* Command without amounts and use the BIN from the truncated PAN in the *Get Amount 3* command to determine if DCC can be used.
- 1-10.14.2.2 C A terminal, where the MSC reader and the MAD handler resides inside the same Secure Device, may extract the BIN from the Track 2 Data. Based on the BIN extracted, the terminal may complete the dialogue concerning DCC, before the *Initiate Payment* command is issued. This flow is shown in figure 1-10.21. This flow may as well be used for Key Entered payments.
- 1-10.14.2.3 A In order to get the BIN for the selected EMV application before the amount is released, the terminal shall use an *Initiate Payment* command without amounts in order to receive a *Get Amount 3* command. It can retrieve the BIN from the truncated PAN of the actual transaction.
- 1-10.14.2.4 A In order to avoid collision between the dialogue concerning DCC and any PIN entry during EMV and MSC transactions, the Accelerated PIN Entry (APE) function shall be disabled. This allows the terminal to handle a DCC dialog before responding the *Get Amount 3* command.

DCC transaction flow

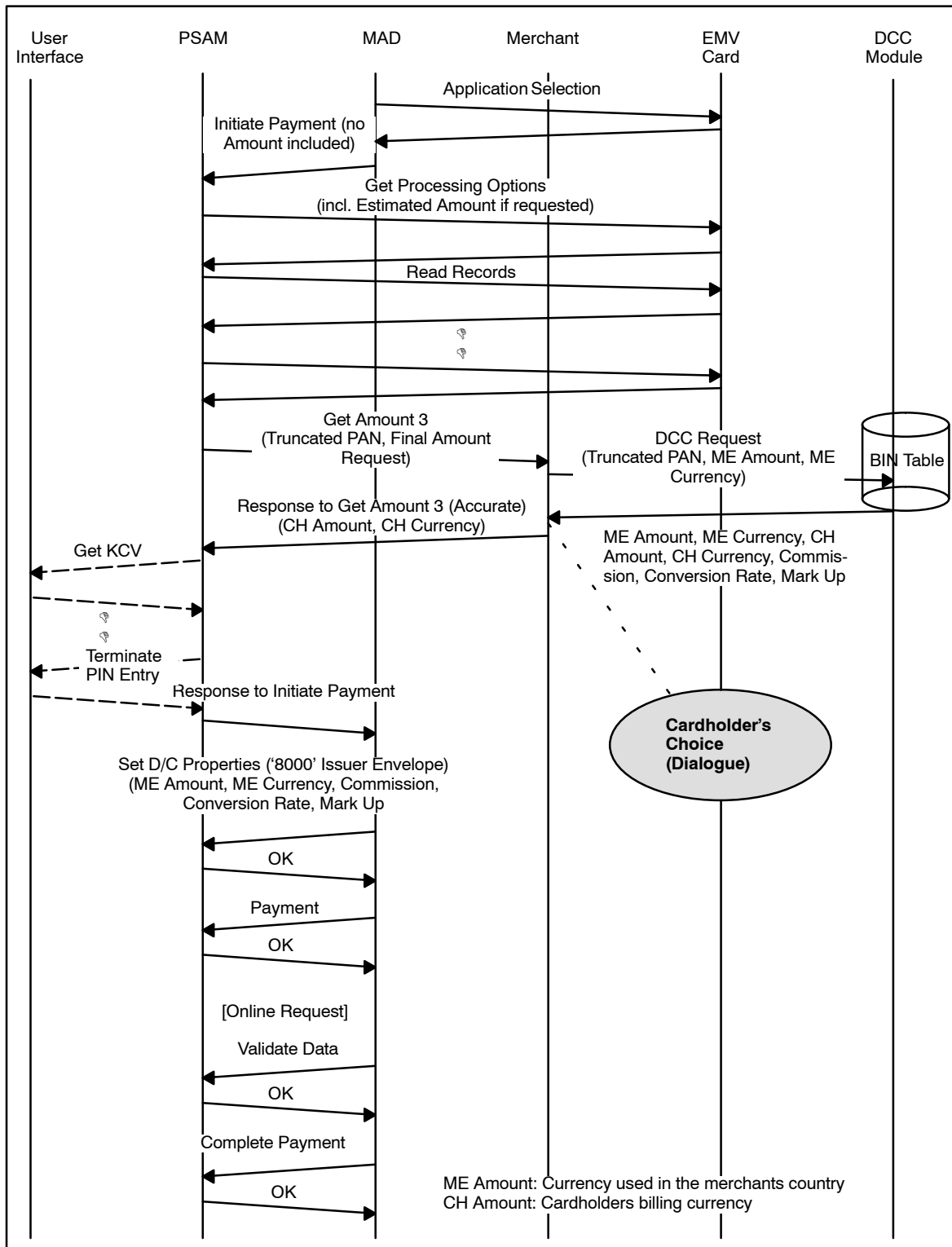


Figure 1-10.19 - DCC flow (APE and DAPE disabled, normal MSC card and EMV card that do not ask for Amount in PDOL)

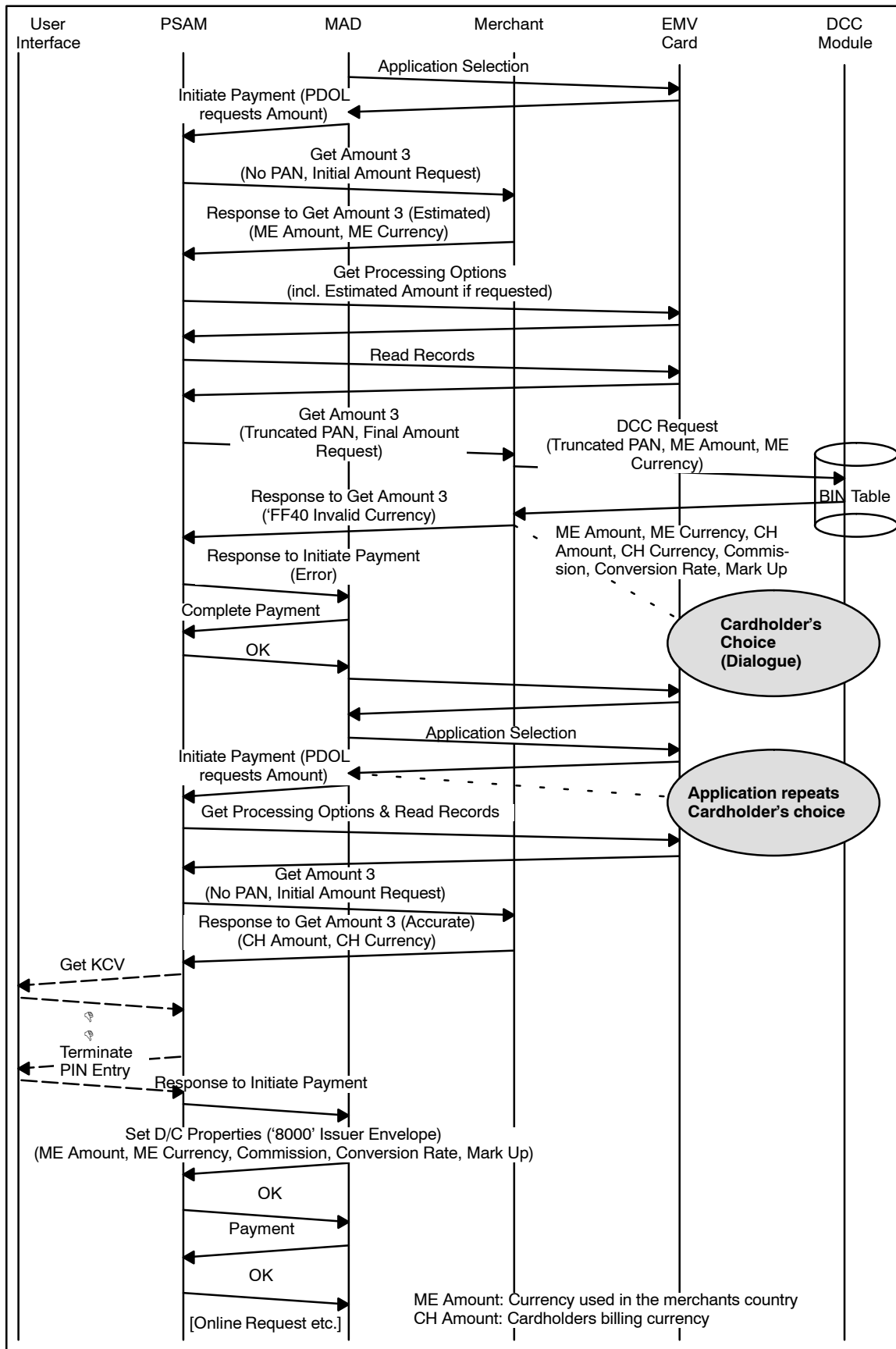


Figure 1-10.20 - DCC flow (APE and DAPE disabled, EMV card that do ask for Amount in PDOL)

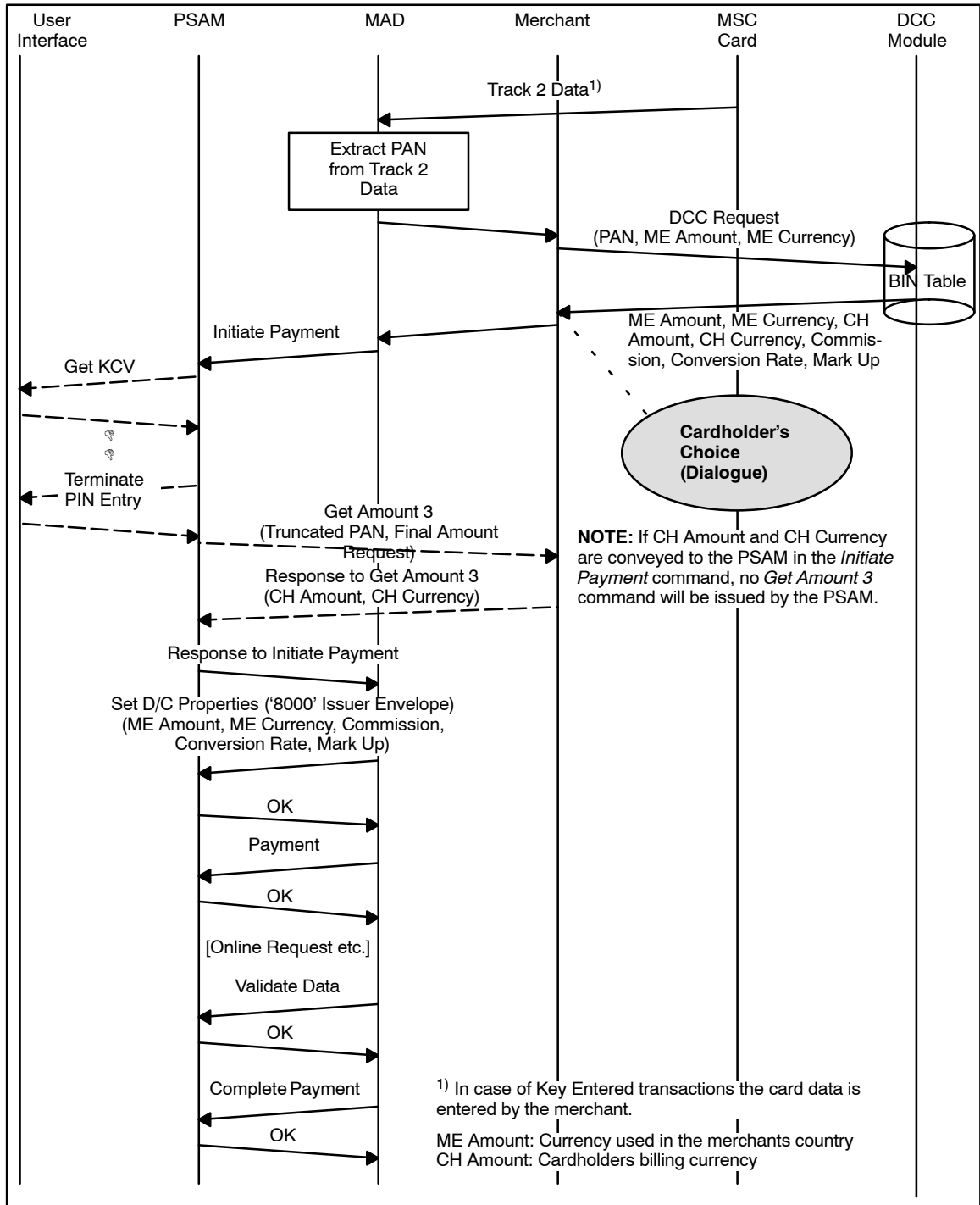


Figure 1-10.21 - DCC flow (MSC/Key Entered, including Fallback from ICC)

NOTE: Figure 1-10.21 is only applicable for Terminals where the BIN is available inside the Secure Device.

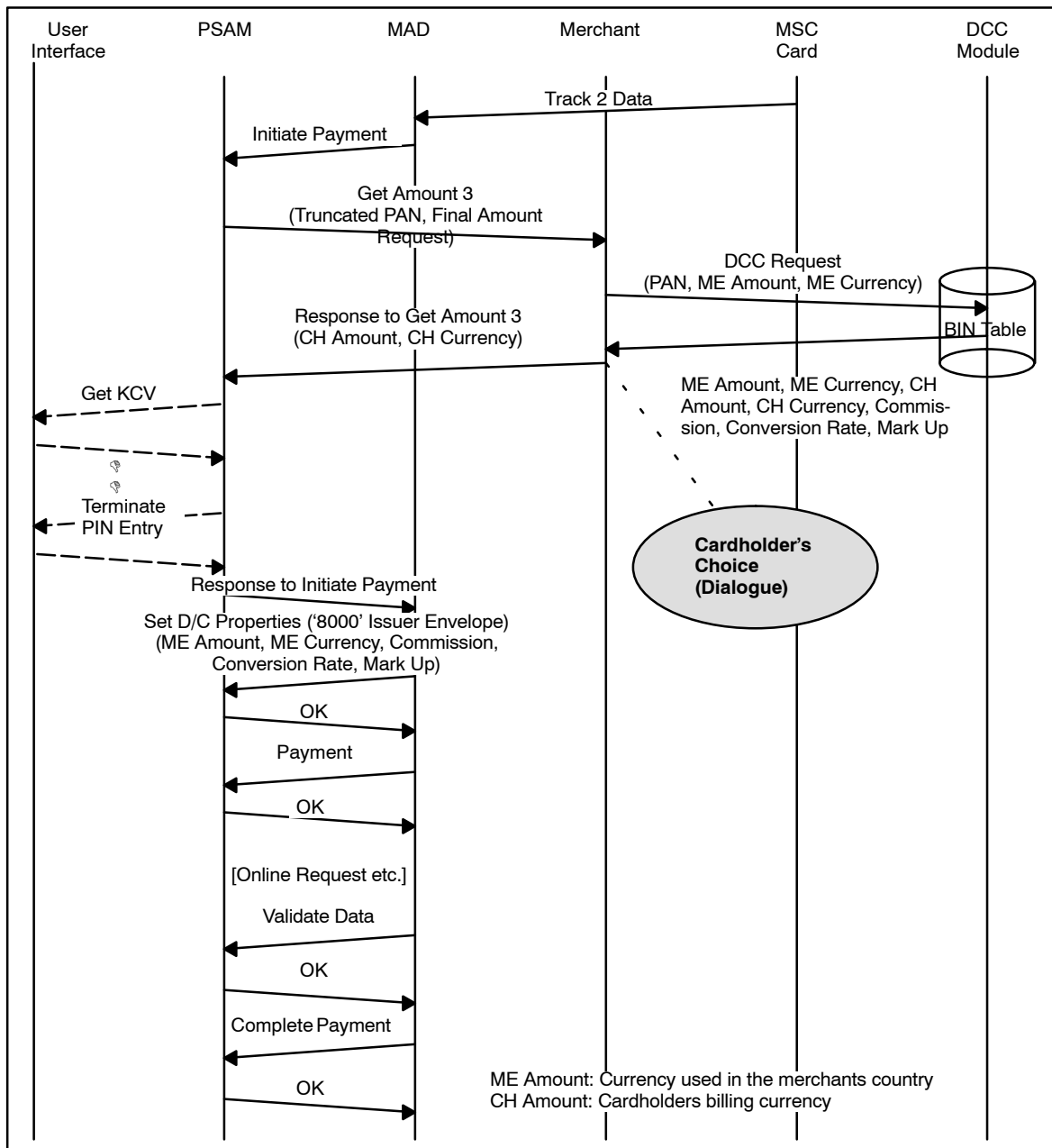


Figure 1-10.22 - DCC flow (MSC card - APE/DAPE disabled, including Fallback)

NOTE: Note that figure 1-10.22 is only applicable for PSAMs supporting disabling of magstripe APE/DAPE.

1-10.14.3 DCC-Transaction-Information

When a DCC is processed, the terminal has to include a number of additional data elements (DCC-Transaction-Information) in the transaction. The additional data makes it possible to differentiate between the currency paid by the cardholder (cardholders billing currency) and the currency posted at the merchant (merchants local currency).

The general transaction data comprises:

- Amount and currency code for the transaction (in case of DCC in the cardholders billing currency)

The additional DCC-Transaction-Information is:

- Amount and currency code in the original currency (merchants local currency)
- Currency conversion rate and Mark Up

This information is handled by the terminal in conjunction with the DCC-application.

- 1-10.14.3.1 A If DCC is chosen, the DCC-Transaction-Information shall be sent in field 47 of the APACS request. If DCC is not chosen, no DCC data shall be sent in field 47.

The PSAM will include the DCC-Transaction-Information in field 47, if any data is received from the terminal by the *Set Debit/Credit Information* command. The detailed requirements are specified in the following sections.

1-10.14.4 Transfer of DCC-Transaction-Information to the PSAM

- 1-10.14.4.1 A The *Set Debit/Credit Properties* command shall be used to convey the DCC-Transaction-Information from the terminal application to the PSAM in the Issuer Envelope data. The PSAM will then include the information in the message(s) conveyed to the acquirer.

- 1-10.14.4.2 A The terminal shall ensure, that **all** Issuer Envelope Data, DCC as well as any non-DCC data, are transferred to the PSAM in one call. See section 1-10.5.1 and section 2-8.5.3 on the use of Issuer Envelope Data.

The format of the *Set Debit/Credit Properties* command and the corresponding response is defined in section 2-14.5.9.

- 1-10.14.4.3 A A Terminal shall ensure that it supports DCC, and that it has a valid exchange rate loaded before it tries to perform a DCC transaction and writes data to the Issuer Envelope. This shall be independent of whether or not a token contains DCC data.

This shall make a terminal not supporting DCC reject a token with DCC data as input.

- 1-10.14.4.4 A For the transfer of DCC-Transaction-Information, the DCC related information shall be:
- The contents of the data element defined in table 1-10.15.

- 1-10.14.4.5 A The total set of Issuer Envelope Data, shall have a header of;
- Identifier = '8000', indicating Issuer Envelope and,
 - LEN_{INFO} = 'nn', indicating the total length of **all** Issuer Envelope Data. (For an envelope only holding DCC information this will be '2A', i.e.42 bytes)

- 1-10.14.4.6 A If the response to the *Set Debit/Credit Properties* command is unsuccessful (ASW1-ASW2 is different from '0000'), the transaction shall be rejected.

- 1-10.14.4.7 A The value of the "DCC indicator" shall be configurable in the terminal. The default value shall be "1".

Table 1-10.15 - DCC data element in DCC-Transaction-Information

Field	Contents	Format	Size (bytes)	Actual Value
TAG _{AdditionalInfo}	Type of Additional Information "ZW"	a2	2	'5A57'
LEN _{AdditionalInfo}	Length of following value fields	b2	2	'0026'
DCC Indicator	DCC algorithm and protocol indicator (value defined by Nets)	n4	2	Note 1
DCC Amount Total (ME)	Total Transaction Amount in merchants local currency, incl. Service, Surcharge and Extra (added by the Cardholder at the time of the transaction)	b4	4	
DCC Amount Goods & Services (ME)	Transaction Amount in merchants local currency, inclusive Services and Surcharges, but exclusive Extra (added by the Cardholder at the time of the transaction)	b4	4	Note 5
DCC Commission (ME)	Additional commission amount in merchants local currency	b4	4	Note 2
DCC CURR (ME)	Currency Code and Exponent of merchants local currency	n6	3	
DCC Reference Exchange Rate	Reference currency exchange rate between merchants local currency and cardholders billing currency	n8	4	
DCC Mark Up Exchange Rate	Mark Up on currency reference exchange rate between merchants local currency and cardholders billing currency	n8	4	
DCC Reference Date	The date related to the reference exchange rate	n8	4	
DCC Commission (CH)	Additional commission amount in cardholders billing currency	b4	4	Note 3
DCC Amount Extra (CH)	Additional amount added by the cardholder in the cardholders billing currency at the time of the transaction, e.g. gratuity	b4	4	Note 4
DCC Waiter ID	ID of the waiter who serviced the cardholder	b1	1	
Total number of bytes (i.e. LEN _{IED} = '2A')			42	

The individual data elements are defined in details in section 2-15.2, "Data Elements for the Debit/Credit Application".

NOTE 1: The data element "DCC Indicator" is used to identify the actual DCC implementation and by this the actual DCC algorithm. The value for "DCC Indicator" is defined by Nets Denmark A/S.

NOTE 2: The use of a fixed DCC commission in the merchants local currency may depend on the business agreements.

NOTE 3: The use of a fixed DCC commission in the cardholders billing currency may depend on the business agreements.

NOTE 4: If DCC is not chosen by the cardholder, the cardholder may add an extra amount in the merchants local currency. In this case the data handling and processing is outside the scope of the present document, since DCC is not involved. No mark up and no commissions shall be included in the calculation of the corresponding extra amount in the merchant local currency. See requirement 1-10.14.5.2 for more information.

NOTE 5: The cardholder may have opted in for Services (e.g. Gratuity) in the merchants currency at a time prior to the transaction. This is documented on the invoice and maybe on the receipt. The amount is part of the DCC Amount for Goods & Services (ME).

NOTE: The “DCC” in front of the DCC relevant data elements will be omitted in the remaining part of this section in order to simply formulas.

1-10.14.5 DCC currency conversion formulas

- 1-10.14.5.1 A The general formula used for computing total transaction amount in the cardholders billing currency shall be as defined below:

$$\begin{aligned} \text{Amount Total (CH)} = & \\ & [[\text{Amount Goods \& Services (ME)} + \text{Commission(ME)}] * \\ & [\text{Reference Exchange Rate} + \text{Mark Up Exchange Rate}]] + \\ & \text{Commission (CH)} + \text{Amount Extra (CH)} \end{aligned}$$

Amount Total (CH) is the total transaction amount in the cardholders billing currency, i.e. the total amount (and currency code) used the transaction according to this specifications.

- 1-10.14.5.2 A Based on the assumption that no Mark Up shall be included, if the cardholders adds an Amount Extra in his/her billing currency, at the time of the transaction, the following formula shall apply for computing the resulting total amount in the merchants local currency (Amount Total (ME)):

$$\begin{aligned} \text{Amount Total (ME)} = & \\ & \text{Amount Goods \& Services (ME)} + \\ & [\text{Amount Extra (CH)} / \text{Reference Exchange Rate}] \end{aligned}$$

Based on the above specified formulas, examples of calculation of amounts and generation of data elements, is shown

in the tables below. There is one calculation, table 1-10.16, for a transaction without gratuity, and one calculation, table 1-10.17 for a transaction with gratuity.

DCC transaction without gratuity (example)

Table 1-10.16 - DCC transaction without gratuity (no Commissions added)

DCC Indicator defined for the actual merchant:	1
<i>DCC Indicator:</i>	'0001'
Merchants local currency:	DKK
<i>DCC CURR (ME):</i>	'020802'
Cardholders billing currency:	EUR
<i>DCC CURR (CH):</i>	'097802'
Amount for goods and services to be paid:	12345,00 DKK
+ Surcharge amount (2%):	246,90 DKK
Transaction amount in merchants local currency (exclusive Extra):	12591,90 DKK
<i>DCC Amount Goods & Services (ME):</i>	'001336B6'
Commission added in merchant local currency (before exchange):	0,00 DKK
<i>DCC Commission (ME):</i>	'00000000'
Exchange rate from DKK to EUR (100,00 EUR = 755,00 DKK):	0,1324503
<i>DCC Reference Exchange Rate:</i>	'71324503'
Mark Up on exchange rate	3%
3% of Exchange rate = 0,03 * 0,1324503	0,003973509
<i>DCC Mark Up Exchange Rate:</i>	'93973509'
The date related to the reference exchange rate:	the 20th of April 2006
<i>DCC Reference Date:</i>	'20060420'
Commission added in cardholders billing currency:	0,00 EUR
<i>DCC Commission (CH):</i>	'00000000'
Based on the values in this example the total transaction amount in the cardholders billing currency, before adding Gratuity should be calculated according to the formula:	
$[[\text{Amount Goods \& Services (ME) + Commission (ME) }] * [\text{Reference Exchange Rate + Mark Up Exchange Rate}] + \text{Commission (CH)}]$ $= [[12591,90 + 0,00] * [0,1324503 + 0,003973509]] + 0,00 =$	
	1717,83 EUR
Gratuity not added by the cardholder:	<not entered>
Total transaction amount in cardholders billing currency:	1717,83 EUR
<i>DCC Amount Extra (CH):</i>	'00000000'
Waiter number:	<not entered>
<i>DCC Waiter ID:</i>	'00'
Transaction amount in merchants local currency (as no extra has been added Extra):	12591,90 DKK
<i>DCC Amount Total (ME):</i>	'001336B6'
Legend: Text in <i>italic</i> shows the representation of the data elements. An explanation of the format of the DCC Mark Up Exchange Rate can be found in section 1-10.14.4.	

DCC transaction with gratuity (example)

Table 1-10.17 - DCC transaction with gratuity (no Commissions and no Mark Up for Extra)

DCC Indicator defined for the actual merchant:	1
<i>DCC Indicator:</i>	'0001'
Merchants local currency:	DKK
<i>DCC CURR (ME):</i>	'020802'
Cardholders billing currency:	EUR
<i>DCC CURR (CH):</i>	'097802'
Amount for goods and services to be paid:	12345,00 DKK
+ Surcharge amount (2%):	246,90 DKK
Transaction amount in merchants local currency (exclusive Extra):	12591,90 DKK
<i>DCC Amount Goods & Services (ME):</i>	'001336B6'
Commission added in merchant local currency (before exchange):	0,00 DKK
<i>DCC Commission (ME):</i>	'00000000'
Exchange rate from DKK to EUR (100,00 EUR = 755,00 DKK):	0,1324503
<i>DCC Reference Exchange Rate:</i>	'71324503'
Mark Up on exchange rate	3%
3% of Exchange rate = 0,03 * 0,1324503	0,003973509
<i>DCC Mark Up Exchange Rate:</i>	'93973509'
The date related to the reference exchange rate:	the 20th of April 2006
<i>DCC Reference Date:</i>	'20060420'
Commission added in cardholders billing currency:	0,00 EUR
<i>DCC Commission (CH):</i>	'00000000'
Based on the values in this example the transaction amount in the cardholders billing currency <u>before</u> adding Gratuity should be calculated according to the this formula:	
$[[\text{Amount Goods \& Services (ME) + Commission (ME) }] * [\text{Reference Exchange Rate + Mark Up Exchange Rate}] + \text{Commission (CH)}]$ $= [[12591,90 + 0,00] * [0,1324503 + 0,003973509]] + 0,00 =$	1717,83 EUR
Gratuity added by the cardholder:	25,00 EUR
Total transaction amount in cardholders billing currency:	1742,83 EUR
<i>DCC Amount Extra (CH):</i>	'000009C4'
Waiter number:	18
<i>DCC Waiter ID:</i>	'12'
Transaction amount in merchants currency exclusive Extra/Gratuity:	12591,90 DKK
<i>DCC Amount Goods & Services (ME):</i>	'001336B6'
Extra/Gratuity amount in the merchants local currency: Notice: The Reference Exchange Rate is used without Mark Up for the exchange of Extra/Gratuity amounts	
$\text{Amount Extra (CH) / Reference Exchange Rate}$ $= 25,00 / 0,1324503 =$	188,75 DKK
Transaction amount in merchants currency including Extra/Gratuity:	12780,65 DKK
<i>DCC Amount Total (ME):</i>	'00138071'
Legend: Text in <i>italic</i> shows the representation of the data elements. An explanation of the format of the DCC Mark Up Exchange Rate can be found in section 1–10.14.4.	

1-10.14.6 Transaction log

See section 1-9.25.6 page 1-9-25, Total Reports and DCC

1-10.14.7 DCC Selection of Currency

General Requirements

- 1-10.14.7.1 A If Dynamic Currency Conversion is relevant for the actual transaction, it shall be decided whether the merchants local currency or the cardholders billing currency is going to be used.
- The way on deciding on the currency to use depends on the type of transaction to be performed.
- 1-10.14.7.2 A For a Purchase or an Original Authorization, the cardholder shall decide whether or not DCC shall be used. The decision shall be based on a dialogue with the cardholder.
- NOTE:** The dialogue may be paper based or display based or a combination.
- 1-10.14.7.3 A The cardholder dialogue shall comply with the requirements defined by MasterCard and Visa for Dynamic Currency Conversion. These requirements do ensure that the cardholder is aware of the conditions before the cardholder makes his/her choice of currency.
- 1-10.14.7.4 C While the cardholder decides whether the transaction shall be a DCC-transaction or normal transaction, the cardholder may have the possibility for adding a gratuity amount.
- 1-10.14.7.5 A If a gratuity amount is added at this step of the transaction processing, the total amount shown to the cardholder during PIN entry and printed on the receipts (including any receipt signed by the cardholder) shall include all relevant additional amounts.
- Gratuity is specified more in detail in section 1-10.15, "Tips".
- 1-10.14.7.6 A For a Supplementary Authorization, the currency shall be the same as used during the Original/Extended Authorization.
- 1-10.14.7.7 A For a Capture, a Cancellation, or a Reversal Authorization the currency to be used shall be the same as in the original transaction.
- 1-10.14.7.8 C For a Refund transaction the currency shall, whenever possible, be the currency of the original transaction. If the original currency cannot be determined, then DCC should not be selected.

DCC selection using pre-receipt

- 1-10.14.7.9 C If the dialogue is paper based, a "pre-receipt" for making the decision about DCC may be presented to the cardholder.
- Since the card must be identified by the terminal before the decision about DCC can be taken, any surcharges will be known too.
- 1-10.14.7.10 C This pre-receipt shall include the amount for goods/service, surcharge (if any) and a total amount.

- 1-10.14.7.11 C The pre-receipt may include free space, making it possible for the cardholder to add gratuity in the currency decided.
- 1-10.14.7.12 C The actual selection may be performed either by the merchant based on the response from the cardholder or by the cardholder based on information presented on the terminal. It shall not be possible to perform the selection process before the pre-receipt has been printed.
- 1-10.14.7.13 A For Refund transactions, the merchant decides the currency to use. No pre-receipt shall be generated and presented to the cardholder.
- 1-10.14.7.14 C A pre-receipt for the merchant may be generated for documentation purpose.

An example of the pre-receipt formats, Receipt CA - CD, can be found in section 1-12.4.32.

DCC selection based on display information

The requirements with respect to cardholder actions during the selection process are;

- The default transaction currency must be the merchant's Pricing Currency
- The cardholder must opt in to the DCC service (DCC must not be the default).

Based on this;

- 1-10.14.7.15 A There shall be a menu where the cardholder can select whether or not to select DCC. The default condition when the menu is displayed shall be that DCC is not selected.
- 1-10.14.7.16 A The customer shall be able to choose between the options and DCC shall not be selected if the cardholder cancels or confirms without further activity.
- 1-10.14.7.17 C The terminal may use the the Cancel and Enter keys in the selection of currency.
- 1-10.14.7.18 A If the Cancel key is activated, once the currency selection is over, the transaction shall be declined.
- 1-10.14.7.19 A The display on the terminal shall show;
- The amount in the merchant's pricing currency.
 - The amount in the cardholders billing currency.
 - The Reference Exchange Rate used.

NOTE: A possible layout could be something like the figure below.

```

                                12345678901234567890
Line 1:  SELECT CURRENCY ☆ ?
Line 2:  AMOUNT: 19160,00 DKK*
Line 3:  AMOUNT: 2568,36 EUR
Line 4:  1 DKK = 0,1340 EUR

```

Figure 1-10.23 - Menu for selecting DCC currency

The arrow keys may be used for selecting the currency. The selected line could be emphasized with a "*" as above, with

inverse text or with text in bold. Activating the green (Enter) key will select the emphasized possibility. Activating the red (Cancel) key will select not to use DCC.

1-10.14.8 DCC transaction types

Information on general receipt formats can be found in section 1-12.1. and information on DCC specific receipt formats can be found in section 1-12.3.3.

DCC receipts and amount values - Purchase

If a pre-receipt has been shown to the cardholder during the dialogue for currency selection, an extra amount may have been added by the cardholder.

Any surcharge added by the merchant may already be part of the transaction amount too.

Therefore the total transaction amount may be divided into the following three sub-amounts:

- Amount for goods and services ("AMOUNT")
- Additional amount added by the merchant ("SURCHARGE")
- Extra amount added by the cardholder, e.g. gratuity ("EXTRA")

Since all relevant amounts will be known before the cardholder approves the transaction by either PIN entry or by signing a receipt, the total transaction amount presented to the cardholder for acceptance can include all additional and extra amounts.

Receipts and amount values - Refund

When a Refund transaction is initiated (as a full or partial reversal of an already performed purchase transaction), the currency selected should be the same as the currency used for the original purchase transaction.

1-10.14.8.1 A If the original purchase transaction was a DCC transaction, the Refund shall be initiated as a DCC transaction too, i.e. the DCC-Transaction-Information shall be filled in for the Refund transaction too.

1-10.14.8.2 A If DCC is an option for the actual card, the terminal shall ask the merchant whether DCC shall be selected or not.

The following situations may be relevant when Refund transactions are initiated:

1. DCC is not relevant for the actual card, for which reason the merchant shall enter the amount using the same currency as the currency used in the original transaction, usually the merchants local currency.
2. DCC is an option for the actual card, for which reason the merchant shall decide whether DCC shall be selected or not. This decision depends on information from the original transaction. Only if the original transaction was a DCC transaction, shall the refund be performed as DCC transaction.

1. If DCC is not selected, the amount shall be entered using the merchants local currency.
2. If DCC is selected, the amount may be entered using either the merchants local currency or the cardholders billing currency. Depending on the currency used, the corresponding amount value in the opposite currency must be computed by the terminal.

An example of the pre-receipt formats for Refund, can be found in section 1-12.4.34.

1-10.14.9 DCC receipt types

Detailed information about the structure of DCC receipts, and examples of DC receipt types can be found in section 1-12.3 "DCC receipt layout".

1-10.15 Transactions with Tips/Gratuity

1-10.15.1 Introduction

1-10.15.1.1 A Addition of Tips/Gratuity (i.e. a cardholder decided extra amount) shall only be an option for the following Business Calls:

- Purchase,
- Capture.

1-10.15.1.2 A The Business Call Capture shall be used only, when the exact amount to pay for goods and services is not known, when the payment sequence is initiated, e.g. at hotels and restaurants (where it shall be possible for the cardholder to add gratuity). If the exact amount is known when the card is presented, Purchase shall be used.

1-10.15.1.3 A Tips/gratuity shall not be an option, if the card data has been key entered.

1-10.15.1.4 C If tips/gratuity is supported by the terminal, the request for any tips/gratuity may be asked by one of the following methods:

- Method 1, adding extra on the invoice.
- Method 2, adding extra on a pre-receipt
- Method 3, using on-display user dialogue
- Method 4, adding extra on the receipt
- Method 5, using request for tips note

NOTE: Regional requirements/constraints may limit the number of methods applicable.

NOTE: The use of method 4 is discouraged as it will be rejected by a large number of new ICC's.

Addition of surcharges

1-10.15.1.5 A Irrespective of the methods used for tips/gratuity, the final amount accepted by the cardholder - either by PIN or signature - shall include any surcharge and tips/gratuity added. No amount shall be added after the cardholder's acceptance.

This gives the following requirements with respect to adding surcharge when tips/gratuity is added.

For method 1, the invoice showing the total for goods and services may include a free field, in which the cardholder is able to add any tips/gratuity, or alternatively write an increased total amount. The tips/gratuity is added on the invoice. Since the means of payment to be used is not known, when tips/gratuity is decided, surcharges shall not be added subsequently.

- 1-10.15.1.6 A If method 1 is used for adding tips/gratuity, surcharges shall not be added.

For method 2, a pre-receipt is printed by the terminal immediately after the card is inserted in the terminal and before the cardholder accepts any amounts. This pre-receipt shows the total amount to pay including any surcharges added. The pre-receipt may include a free field, in which the cardholder is able to add any tips/gratuity, or alternatively write an increased total amount. The pre-receipt may be a combined DCC and tips/gratuity pre-receipt, if both functions are relevant for the actual transaction. After the cardholder has accepted the pre-receipt and maybe added tips/gratuity, the transaction sequence continues.

For method 3, a dialogue between the cardholder and the terminal is initiated immediately after the card is inserted in the terminal, and before the cardholder accepts any amounts. The cardholder is guided through a sequence of questions for the decision about any tips/gratuity. The amount including surcharges is known. After the dialogue is completed, the amount for tips/gratuity will be known, and the transaction sequence may continue.

Method 4 is similar to the 'old' signature and magnetic stripe transactions. These are signature based transactions, where any surcharges is know in advance.

- 1-10.15.1.7 C If method 2, 3 or 4 is used for adding tips/gratuity, any surcharges based on the actual means of payment is known in advance and will be presented to the cardholder, before the cardholder decides any tips/gratuity. Surcharges may be added for these methods.

If method 5 is used for adding tips/gratuity, the cardholder shall be advised that surcharges may be added, when the cardholder decides the value for tips/gratuity. The exact surcharge amount will not be known, but the relevant rates shall be presented to the cardholder.

- 1-10.15.1.8 A If method 5 is used, surcharges shall only be added to the amount covering goods and services. Surcharges shall not be added to the tips amount specified by the cardholder.

1-10.15.2 Method 1, Tips on invoice

As the tips are added before the terminal is activated, the requirement for this is outside the scope of the current document.

1-10.15.3 Method 2, Tips on pre-receipt

- 1-10.15.3.1 C The terminal may be able to generate a pre-receipt. The pre-receipt may combine addition of tips/gratuity and the selection of DCC.

- 1-10.15.3.2 A The structure of a pre-receipt shall be as specified in section 1-12.3.2 figure 1-12.12.

1-10.15.4 Method 3, Tips on display

It is possible to handle the entry of tips directly on the terminal, using the display and the keyboard. This is possible on a terminal with a separate cardholder display and as well as on a terminal with a combined display.

Transaction flow

On-terminal entry of tips is inserted in the flow between the state where the cardholder inserts the card into the terminal, and the state where the card validation is performed, e.g. while the PSAM awaits the amount. The flow of the transaction could consist of the following steps;

1. The Merchant selects the type of transaction to perform (Purchase) and the amount.
2. The card is inserted into the terminal.
3. If the terminal is a Single Unit Terminal, SUT, the terminal should prompt the Merchant to hand over the terminal to the cardholder.
4. The terminal request whether or not the cardholder wants to add tips to the amount, see figure 1-10.24. If the cardholder confirms then continue with the next step, else skip to step 8 of this flow.
5. The Purchase amount including any fees/surcharges, is displayed on the terminal, see figure 1-10.25. The cardholder is requested to enter the total amount, i.e. the sum of the purchase amount and any extras/tips. If the cardholder just confirms the amount without entering any new total, then the terminal continues to step 8 in this flow, indicating that no tips entered.
6. The terminal verifies that the total amount is as least the purchase amount including any fees/surcharges. If the total amount is too small, the terminal displays an error message as shown on figure 1-10.26. The error message is displayed for at least 6 seconds and the terminal returns to step 8 of this flow. The terminal continues with the next step if the total amount is large enough.
7. The terminal calculates the extra/tips amount. The terminal displays the following three amounts; the purchase amount, the extras/tips and the total amount as shown on figure 1-10.27. The cardholder is requested to confirm the amount. If the cardholder declines, then return to step 4 of this flow else continue.
8. The terminal continues with the normal card validation flow.

Examples of display texts

The structure of the different display texts is shown below.

Select addition of tips - step4

```

12345678901234567890
Line 1:  ADD EXTRA / TIPS?
Line 2:
Line 3:  YES=GREEN / NO=RED
Line 4:

```

```

12345678901234567890
Line 1:  TILFØJ DRIKKEPENGE?
Line 2:
Line 3:  JA=GRØN / NEJ=RØD
Line 4:

```

Figure 1-10.24 - Menu for selecting to add gratuity/tips

NOTE: The method shown for selection between to confirm and to decline an action is but one possibility. The actual method used may be terminal implementation dependent.

Entry of total amount - step 5

```

12345678901234567890
Line 1:  SPECIFY TOTAL AMOUNT
Line 2:
Line 3:  AMOUNT:123456,78 EUR
Line 4:  TOTAL: _____ EUR

```

```

12345678901234567890
Line 1:  INDTAST TOTALBELØB
Line 2:
Line 3:  AMOUNT:123456,78 DKK
Line 4:  TOTAL: _____ DKK

```

Figure 1-10.25 - Menu for entering total amount

NOTE: The default behavior, i.e. just confirming without entering any amount, is that no tips are added.

Detecting amount too small - step 6

```

12345678901234567890
Line 1: TOTAL LESS THAN
Line 2: PURCHASE AMOUNT.
Line 3:
Line 4: REENTER TOTAL AMOUNT

```

```

12345678901234567890
Line 1: TOTALBELØB MINDRE
Line 2: END KØB.
Line 3: GENDINDTAST TOTAL-
Line 4: BELØB

```

Figure 1-10.26 - Message at a too small total amount

Confirming total amount - step 7

```

12345678901234567890
Line 1: AMOUNT:123456,78 EUR
Line 2: EXTRA: 543,22 EUR
Line 3: TOTAL: 124000,00 EUR
Line 4: YES=GREEN / NO=RED

```

```

12345678901234567890
Line 1: BELØB: 123506,78 DKK
Line 2: EXTRA: 493,22 DKK
Line 3: TOTAL: 124000,00 DKK
Line 4: JA=GRØN / NEJ=RØD

```

Figure 1-10.27 - Menu for confirming gratuity/tips

Requirements

The flow as described above causes the following requirements.

- | | | |
|-------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-10.15.4.1 | C | The terminal may have capabilities for on-terminal handling of the entry of gratuity/tips using the display and keypad on the terminal. |
| 1-10.15.4.2 | A | The on-terminal entry of tips shall, if the terminal does not support DCC, start after the card has been swiped/inserted into the terminal. |
| | | NOTE: The entry of cardholder information on the Cardholder keyboard at this stage of the transaction inhibits the use of APE/DAPE on the terminal. |
| 1-10.15.4.3 | A | The on-terminal entry of tips shall, if the terminal supports DCC, start after the cardholders selection of currency. |

- 1-10.15.4.4 B The terminal should, if the terminal is a Single Unit Terminal, prompt the Merchant to hand over the terminal to the cardholder for entry of tips at this stage of the transaction.
- NOTE:** More information about requirements for Single Unit Terminals, can be found in section 1-13 of this document.
- 1-10.15.4.5 A The on-terminal entry of tips shall be completed before the card validation starts and PIN entry is enabled (in case of PIN being selected as CVM).
- 1-10.15.4.6 C The terminal may use the the Cancel and Enter keys in the selection of adding tips.
- 1-10.15.4.7 A If the Cancel key is activated, once the tips selection is over, the transaction shall be declined.
- 1-10.15.4.8 A The terminal shall not support addition of tips after the card validation, if on-terminal entry of tips has been used.
- 1-10.15.4.9 A The terminal shall start the on-terminal entry of tips by asking whether or not the cardholder wants to add tips.
- 1-10.15.4.10 A The terminal shall terminate the entry of tips, if the cardholder declines to add tips.
- 1-10.15.4.11 C Adding tips may be performed either by entering the tips amount, or by entering the total amount.
- 1-10.15.4.12 C Selection between entry of tips and entry of total amount may be a configuration parameter for the terminal
- 1-10.15.4.13 A If the entry of the total amount is used the terminal shall present a display requesting the cardholder to enter a total amount. The display shall as well show the purchase amount including any fees/surcharges. The cardholder shall be able to enter a total amount on this display.
- 1-10.15.4.14 A If the entry of the tips amount is used the terminal shall present a display requesting the cardholder to enter a tip amount. The display shall as well display the purchase amount including any fees/surcharges. The cardholder shall be able to enter a tip amount on this display.
- 1-10.15.4.15 A The terminal shall, if the cardholder does not enter a new total or tip but just confirms by pressing the 'Enter' button, continue as if no tip/extra is added.
- 1-10.15.4.16 A The cardholder shall at this stage be able to decline the entry of tips by using the 'Cancel' button. This shall cause the terminal to revert to the state asking the cardholder if he want to add tips.
- 1-10.15.4.17 A The terminal shall, if a total amount is entered, verify that the total amount entered is at least as large as the purchase amount including any fees. The terminal shall, if the amount is too low, display a correction message to the cardholder and request that a new total amount is entered.
- 1-10.15.4.18 A The correction message shall stay on the display for at least 6 second or until the cardholder confirms the message. The terminal shall then revert to the display requesting the (re)entry of the total amount.

- 1-10.15.4.19 A The terminal shall, when a valid total or tips amount has been entered, display the purchase amount, the extras and the total amount and ask the cardholder to confirm the amount. The terminal shall revert to the state of entering tips, if the cardholder declines the action. The terminal shall continue with the card verification if the cardholder confirms the action.
- 1-10.15.4.20 C The terminal should, if it is a Single Unit Terminal and Signature is used as CVM, prompt the cardholder to return the terminal to the Merchant before continuing with the card verification.

1-10.15.5 Method 4, Tips on receipt

Method 4 covers the use of tips in restaurants where a tips amount may be added after the cardholder has approved the transaction. The basic market segment for this method is the restaurant environment.

Since this method is based on signature based transactions only, the default principles for CVM selection is overruled by forcing signature. Since the terminal is PIN capable, but the default use of PIN has been overruled, the ICC or the issuer may reject the transaction. In case of any subsequent complaints from the issuer, the transaction may be nullified (charge back), due to the overruling of the preferred CVM.

NOTE: The use of this method is discouraged. A large number of the cards being issued now will reject the use of this transaction type based on forced signature.

Transaction flow

The flow described in this section is based on the assumption that the amount to pay for goods and services is known, when the payment process is initiated. During the payment process, any surcharge (depending on the actual card) may be added, like the cardholder may be able to add any tips/gratuity.

The basic market segment for such a terminal is the restaurant environment. Therefore this segment is used as an example in this document, but the implementation may also be relevant for other environments with similar demands.

The following steps describes the general transaction sequence:

1. A (pre-)authorization is initiated, based on the amount to pay for goods and services and the cardholders card.
2. The Token received as output from the (pre-)authorization is stored by the terminal.
3. A receipt is printed. The cardholder may be able to add tips/gratuity on the receipt. The receipt shall be signed by the cardholder.
4. When the cardholder has signed the receipt, the merchant completes the payment sequence by initiating a capture on the terminal.
5. The Token from the (pre-)authorization together with the final transaction amount (including any tips/gratuity) is used as input to the capture.

Requirements

- 1-10.15.5.1 A Due to the preferred transaction flow, signature has to be used as the primary Cardholder Verification Method (CVM). To be able to select signature as the primary CVM, the transaction shall be initiated as "Forced Signature Transactions".
- 1-10.15.5.2 A When the cardholder has confirmed the amount in connection with PIN entry, no subsequent additions shall be possible. Therefore PIN shall not be an option in combination with 'late addition' of tips/gratuity.
- NOTE:** Since the transaction flow described does not correspond to the "Chip and PIN" business procedures recommended by the card schemes, the method described in this document may only be acceptable for a limited period of time.
- The individual card issuers may configure their cards differently. The parameters defined in the cards may not accept the use of "forced signature", when the card is used in a terminal with PIN capability. The card schemes recommend different parameter combinations depending on the actual card brand. It is expected that more and more chip cards will reject technically, when a "forced signature" transaction is initiated.
- 1-10.15.5.3 A Due to both the business and technical issues when "forced signature" is used, any terminals supporting the functions described in this document shall as well support at least one of the three methods for requesting tips/gratuity before the online authorization is initiated.
- To be able to implement method 4, a payment sequence based on a flow similar to the flow used in previous generations of terminals, the transaction flow in the Chip Terminal must be based on Tokens.
- 1-10.15.5.4 A A Token Macro Function "AUTHORIZE FOR TIPS" specified in section 1-10.12.7 shall be initiated when both the amount to pay for goods and services, and the actual payment card are available.
- 1-10.15.5.5 A When the cardholder has signed the receipt, and maybe added any tips/gratuity, the merchant shall complete the payment sequence by the Token Macro Function "FINALIZE WITH TIPS" specified in section 1-10.12.7. The merchant shall initiate the function irrespective of the tips/gratuity amount. If the merchant does not complete this step, the merchant will not receive any money.
- 1-10.15.5.6 A To be sure that the financial transaction generated during the Token Macro Function "FINALIZE WITH TIPS" is build on the correct date and time information etc., this function shall be initiated in continuation of the cardholder signing the receipt.

1-10.15.6 Method 5, Tips before the card is known

Method 5 covers entry of tips before the card is known. When the merchant hands over the invoice, a request-for-tips-note may be attached. The request-for-tips-note may be printed by the card terminal. The request-for-tips-note will not show any card details (the card has not been presented yet), but the total amount shall appear. The request-for-tips-note will include a field, in which the cardholder is able to add any tips/gratuity, and the actual surcharge rates may be also be included on the note. The cardholder will not know the exact value added as surcharge, when tips is added, but a note will inform the cardholder that surcharge will be added. This makes it acceptable to add surcharge after the cardholder has added any tips/gratuity.

Transaction flow

The flow described is intended for use in restaurants or similar environments where tips is an option.

1. When the invoice is added up, the waiter hands over the invoice to the customer. When the invoice is handed over, the means of payment is not known.
2. Together with the invoice a request-for-tips note may be enclosed. The note is intended to request for tips/gratuity.
3. If the customer decides to pay by card, the customer may add an extra amount on the request-for-tips-note and hand over the note together with the payment card.
4. The request-for-tips-note states that surcharge may be added. The actual surcharge rates appears on the note too.
5. The waiter will initiate a Purchase procedure based on the actual amount and the actual card.
6. During the Purchase procedure the type of payment card will be identified by the terminal, and the actual surcharge will be calculated and added before the cardholder accepts the final amount.

Requirements

1-10.15.6.1	C	The terminal may be able to generate a request-for-tips note.
1-10.15.6.2	C	The invoice showing the total for goods and service, and the request-for-tips-note may be combined as one single document.
1-10.15.6.3	C	The request-for-tips-note shall show the total amount for goods and services.
1-10.15.6.4	A	The request-for-tips note shall follow the structure of a pre-receipt as specified in section 1-12.2.14 "Pre-receipt".
1-10.15.6.5	A	The request-for-tips-note shall include information on surcharges as stated in section 1-12.2.10. This includes requirement 1-12.2.10.13 - 1-12.2.10.15 for pre-receipt where the card is not known.

-
- 1-10.15.6.6 A The request-for-tips-note shall show the rates for the actual merchant, and all rates shall appear together with the corresponding card scheme names.
- 1-10.15.6.7 A When the payment card is presented to the merchant, the transaction processing shall be based on the Purchase function.
- 1-10.15.6.8 A Surcharge shall only be added to the amount covering goods and services.
- 1-10.15.6.9 A Surcharge shall not be added to the tips amount specified by the cardholder.
- 1-10.15.6.10 A Any tips/gratuity added shall be included when the cardholder accepts the final amount.
- 1-10.15.6.11 A The cardholder shall accept the the final amount by either PIN or signature.

1-11 Display Texts

1-11.1 Introduction

This section defines the texts to be displayed if the terminal supports 20 characters per line and as well as the texts if the terminal only is capable of displaying 16 characters per line.

In the initial sections, messages are defined for the default languages, English and Danish.

The text to be used in other languages are to be found in section 1-15 page 1-15-1, Regional Requirements and following, different regional requirements.

The table of message text id is followed by a number of examples on how the message flow on the User Interface Display shall be implemented.

At the end of the section is an overview of recommended texts to use for business calls and administrative functions.

1-11.1.1 Language Requirements

In the local markets, the cardholder expects to see local language used in the display and receipt texts.

- 1-11.1.1.1 A The terminal shall at least be able to use the local language for display and receipt texts.

NOTE: This is a requirement in ref. 20: "EMV ICC Specification", Book 4, section 11.1.

- 1-11.1.1.2 B The terminal shall support the ISO 8859 character set, see ref. 12: "ISO/IEC 8859-15", needed for displaying the texts in the local language.

NOTE: In some countries, the character set may be simplified according to normal practise in each country.

1-11.1.2 Combined Approval of Amount and PIN

On terminals developed according to this specification, the cardholder presses the Enter button only once for approval of both the amount and the PIN.

NOTE: Separate approval of amount and PIN is not possible on terminals complying with this specification.

NOTE: Accelerated PIN Entry, APE, may, in some environments, be used in order to facilitate parallel processing and thereby speeding up the overall payment process. See section 1-9.13.1.

1-11.2 Messages for Display

In this section, Messages for Display are defined. The section contains the EMV and TAPA defined Message identifiers as well as the text in English.

NOTE: The Danish version of this table is now moved to the Regional Requirements, section 1-15.2.

The texts in table 1-11.1 are designed for a display capable of displaying at least 20 characters per line and 16 characters per line, respectively.

Table 1-11.1 - Messages for Display

Message Code	20 Characters Display		16 Characters Display	
	English	National	English	National
'01'	(Amount)		(Amount)	
'02'	(Amount) OK?		(Amount) OK?	
'03'	Approved		Approved	
'04'	Call Your Bank		Call Your Bank	
'05'	Cancel or Enter		Cancel or Enter	
'06'	Card Error		Card Error	
'07'	Declined		Declined	
'08'	Enter Amount		Enter Amount	
'09'	Enter PIN		Enter PIN	
'0A'	Incorrect PIN		Incorrect PIN	
'0B'	Insert Card		Insert Card	
'0C'	Not Accepted		Not Accepted	
'0D'	PIN OK		PIN OK	
'0E'	Please Wait		Please Wait	
'0F'	Processing Error		Processing Error	
'10'	Remove Card		Remove Card	

Table 1-11.1 - Messages for Display (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'11'	Use Chip Reader		Use Chip Reader	
'12'	Use MAG Stripe		Use MAG Stripe	
'13'	Try Again		Try Again	
'14'	Welcome		Welcome	
'15'	Present Card		Present Card	
'16'	Processing		Processing	
'17'	Card read OK. Please remove card		Card read OK Remove card	
'18'	Insert or swipe card		Insert/swipe crd	
'19'	Use one card only		One card only	
'1A' – '3F'	RFU for assignment by EMV			
'40'	System Error, retry		System Error	
'41'	Invalid Card		Invalid Card	
'42'	Card out-of-order		Error in card	
'43'	Expired Card		Expired Card	
'44'	Insufficient value		Too low value	
'45'	Card not present		Card missing	
'46'	Data Store full		Data Store full	
'47'	Timed out		Timed out	
'48'	Thank You		Thank You	
'49'	Not available		Not available	
'4A'	Print receipt?		Print receipt?	
'4B'	Cancel		Cancel	
'4C'	Make Selection		Make Selection	
'4D'	Incorrect Amount		Wrong Amount	
'4E'	Welcome		Welcome	
'4F'	Signature		Signature	
'50'	Application Menu		Menu	
'51'	Transaction Menu		Menu	
'52'	Purchase		Purchase	
'53'	Page		Page	
'54'	PIN Blocked		PIN Blocked	
'55'	Enter New PIN		Enter New PIN	
'56'	PIN Changed		PIN Changed	
'57'	PIN Unchanged		PIN Unchanged	
'58'	2 PINs not same		2 PINs not same	
'59'	Confirm new PIN		Confirm new PIN	

Table 1-11.1 - Messages for Display (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'5A'	Change PIN		Change PIN	
'5B'	Unblock PIN		Unblock PIN	
'5C'	PIN not blocked		PIN not blocked	
'5D'	PIN Unblocked		PIN Unblocked	
'5E'	Calling...		Calling...	
'5F'	Transmitting...		Transmitting...	
'60'	Receiving...		Receiving...	
'61'	Comms Error		Comms Error	
'62'	Disconnecting		Disconnecting	
'63'	Trans Log Upload		Trans Log Upload	
'64'	Retrying		Retrying	
'65'	Upload Done		Upload Done	
'66'	Upload Failed		Upload Failed	
'67'	No Records		No Records	
'68'	Debit:		Debit:	
'69'	Credit:		Credit:	
'6A'	Credit Reversal		Credit Reversal	
'6B'	Cash Load		Cash Load	
'6C'	Balance:		Balance:	
'6D'	New Balance		New Balance	
'6E'	Specify Amount		Specify Amount	
'6F'	Recovery Needed		Recovery Needed	
'70'	Insufficient Funds		Value too high	
'71'	Recovery Failed		Recovery Failed	
'72'	Recovery Done		Recovery Done	
'73'	Money Taken		Money Taken	
'74'	Show Balance		Show Balance	
'75'	Statement Review		Statement Review	
'76'	by issuer		by issuer	
'77'	Upload Time		Upload Time	
'78'	Start (HH:MM)		Start (HH:MM)	
'79'	End (HH:MM)		End (HH:MM)	
'7A'	Prefix Nr		Prefix Nr	
'7B'	Totals		Totals	
'7C'	Auth X25 No		Auth X25 No	
'7D'	Upload X25 No		Upload X25 No	
'7E'	No Trials:		No Trials:	
'7F'	Delay:		Delay:	
'80'	Onl Auth. Data		Onl Auth. Data	

Table 1-11.1 - Messages for Display (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'81'	Onl Upload Data		Onl Upload Data	
'82'	Get Cash		Get Cash	
'83'	Unblock Appli.		Unblock Appli.	
'84'	Pre-Autho.		Pre-Autho.	
'85'	Pre Completion		Pre Completion	
'86'	Refund:		Refund:	
'87'	Cancellation		Cancellation	
'88'	D/C Menu		D/C Menu	
'89'	Precomp. Number		Precomp. Number	
'8A'	Get Merchant PIN		Get Merchant PIN	
'8B'	Data required in the DB		Need data in DB	
'8C'	Interval (MM)		Interval (MM)	
'8D'	Number Attempts		Number Attempts	
'8E'	Load Stop List		Load Stop List	
'8F'	Pick up Card		Pick up Card	
'90'	Denied:		Denied:	
'91'	View Balance?		View Balance?	
'92'	Do not honor		Do not honor	
'93'	Expired Card		Expired Card	
'94'	Suspected fraud		Suspected fraud	
'95'	PIN exceeded		PIN exceeded	
'96'	Refer Issuer		Refer Issuer	
'97'	No card number		No card number	
'98'	Excessive Amount		Excessive Amount	
'99'	Counterfeit Card		Counterfeit Card	
'9A'	Format Error		Format Error	
'9B'	Card issuer or		Card issuer or	
'9C'	Switch inop.		Switch inop.	
'9D'	Bad Routing		Bad Routing	
'9E'	Sys malfunction		Sys malfunction	
'9F'	Yes		Yes	
'A0'	No		No	
'A1'	Capture Card		Capture Card	
'A2'	Money not taken		Money not taken	
'A3'	Exp. date (YYMM)		Exp. date (YYMM)	
'A4'	Enter PAN		Enter PAN	
'A5'	Enter Term ID		Enter Term ID	

Table 1-11.1 - Messages for Display (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'A6'	Params Required		Params Required	
'A7'	Forced online		Forced online	
'A8'	Sale:		Sale:	
'A9'	Refund:		Refund:	
'AA'	Purse empty		Purse empty	
'AB'	Set currency		Set currency	
'AC'	Currency changed		Currency changed	
'AD'	Terminal ID		Terminal ID	
'AE'	Exceeds limit		Exceeds limit	
'AF'	Invalid currency		Invalid currency	
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready		Terminal ready	
'E1' 1)	No receipt		No receipt	
'E2'				
'E3'	Error reading card		Card read error	
'E4'	Card validated		Card validated	
'E5'	Receipt wanted?		Receipt wanted?	
'E6'	Printing receipt		Printing receipt	
'E7'	Purchase interrupted		Purchase stopped	
'E8'	Terminal failure		Terminal failure	
'E9'	Terminal busy		Terminal busy	
'EA'	Out of order		Out of order	
'EB'	Push		Push	
'EC'	Enter PIN and Accept		Enter PIN/Accept	
'ED'	Swipe card		Swipe card	
'EE'	Insert card again		Insert card	
'EF'	PIN:		PIN:	
'F0'	Buy:		Buy:	
'F1'	Accept?		Accept?	
'F2'	Bonus added		Bonus added	
'F3'	Technical failure		Tech. failure	
'F4'	Try again later		Try again later	
'F5'	Limit reached		Limit reached	
'F6'	Card is blocked		Card is blocked	
'F7'	Refer Acquirer		Refer Acquirer	
'F8'	(X) PIN tries left		(X) PIN tries left	
'F9'	Invalid merchant		Invalid merchant	
'FA'	Card unknown		Card unknown	

Table 1-11.1 - Messages for Display (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'FB'	Split payment?		Split payment?	
'FC'	Card/amount re-corded		Data recorded	
'FD'	Identical purchase		Identical trans.	
'FE'	(Action Code)		(Action Code)	
'FF'	Invalid transaction		Invalid trans.	

Legend: ¹⁾ The message may flash on the display to attract the cardholder's attention.
²⁾ A “-” or a “+” may be used instead of the “/”.
Generally, when “(“and”) are used, the actual value of whatever is inside the brackets is indicated.
(X) indicates actual value.
Message Codes 'EC' and 'F1' are proposed text

1-11.3 Display flow for Transactions

Section 2-6.2.5 page 2-6-4 defines the requirements to the User Interface Display.

In the current section, a number of transaction examples are used to define the use of the User Interface Display using the English texts. The corresponding Message Code, MC, is shown next to the display line. Translation to other languages ca be obtained by looking up the MC for the corresponding language.

It is assumed that the User Interface Display used, is able to display at least 4 lines of each 20 characters. It is also assumed that requirement 2-4.8.1.11 page 2-4-13 is not implemented.

The user interface for contactless transactions is described in ref.22 : “EMVCo Contactless Specifications for Payment Systems, Book B, Entry Point Specification”.

1-11.3.1 Example 1: Display flow PIN Trans. - Approved

This example is based on 'Combined PIN Entry and Amount Confirmation'.

Step 1 - PIN Entry enabled but Amount not available yet

	12345678901234567890	
Line 1:		
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Enter PIN	MC = '09'

Figure 1-11.1 - PIN entry enabled but Amount not available yet

Step 2 - PIN Entry enabled and Amount available

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Enter PIN and Accept	MC = 'EC'

Figure 1-11.2 - PIN entry enabled and amount available

Step 3 - PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.3 - PIN entry completed and Amount accepted, waiting for Validation

Step 4 - Validation completed, Transaction approved

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:	Approved	MC = '03'
Line 4:		

Figure 1-11.4 - Validation completed, Transaction approved

1-11.3.2 Example 2: Display flow PIN Trans. - PIN Error

This example is based on 'Combined PIN Entry and Amount Confirmation'.

Step 1 - PIN Entry enabled but Amount not available yet

	12345678901234567890	
Line 1:		
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Enter PIN	MC = '09'

Figure 1-11.5 - PIN entry enabled but Amount not available yet

Step 2 - PIN Entry enabled and Amount available

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Enter PIN and Accept	MC = 'EC'

Figure 1-11.6 - PIN Entry enabled and Amount available

Step 3 - PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.7 - PIN Entry completed and Amount accepted, waiting for Validation

Step 4 - Validation completed, Transaction rejected - PIN Error

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:	Declined	MC = '07'
Line 4:	Incorrect PIN	MC = '0A'

Figure 1-11.8 - Validation completed, Transaction rejected - PIN Error

1-11.3.3 Example 3: Display flow PIN Trans. - PIN Retry

This example is based on 'Combined PIN Entry and Amount Confirmation'.

Step 1 - PIN Entry Enabled but Amount not available yet

	12345678901234567890	
Line 1:		
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Enter PIN	MC = '09'

Figure 1-11.9 - PIN entry enabled but Amount not available yet

Step 2 - PIN Entry Enabled and Amount available

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Enter PIN and Accept	MC = 'EC'

Figure 1-11.10 - PIN entry enabled and Amount available

Step 3 - PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.11 - PIN entry completed and Amount accepted, waiting for Validation

Step 4 - Validation completed, Transaction rejected - PIN Error (Texts are displayed for 6 seconds)**NOTE:** This step may be skipped.

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:	Declined	MC = '07'
Line 4:	Incorrect PIN	MC = '0A'

Figure 1-11.12 - Validation completed, Transaction rejected - PIN Error

Step 5 - Validation completed, Transaction rejected - PIN Error - (Remaining PIN attempts available - PIN Retry)**NOTE:** If the number of PIN tries left is not displayed, line 3 may remain blank or the remaining information may be rearranged.

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN:	MC = 'EF' + an "*" for each digit entered
Line 3:	(X) PIN tries left	MC = 'F8', (X) indicates the number of PIN tries left
Line 4a:	Incorrect PIN	MC = '0A', alternating between line 4a and 4b
Line 4b:	Enter PIN and Accept	MC = 'EC', alternating between line 4a and 4b

Figure 1-11.13 - Validation completed, Transaction rejected - PIN Error - (Remaining PIN attempts available - PIN Retry)

Step 6 - When Cardholder enters the first Digit

12345678901234567890		
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *	MC = 'EF' + an "*" for each digit entered
Line 3:	(X) PIN tries left	MC = 'F8', (X) indicates the number of PIN tries left
Line 4:	Enter PIN and Accept	MC = 'EC'

Figure 1-11.14 - When the cardholder enters the first PIN Digit

Step 7 - PIN Entry completed and Amount accepted, waiting for Validation

12345678901234567890		
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.15 - PIN Entry Completed and Amount accepted, waiting for Validation

1-11.3.4 Example 4: Display flow Signature Trans. - Approved

This example is based on 'No Amount Acceptance'.

Step 1 - Amount available, waiting for Validation

12345678901234567890		
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.16 - Amount available, waiting for Validation

Step 2 - Validation completed, Transaction approved

12345678901234567890		
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:	Approved	MC = '03'
Line 4:		

Figure 1-11.17 - Validation completed, Transaction approved

1-11.3.5 Example 5: Display flow Signature Trans. - Approved

This example is based on 'Amount Acceptance'.

Step 1 - Amount available, waiting for Cardholder Acceptance

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:		
Line 4:	Accept?	MC = 'F1'

Figure 1-11.18 - Amount available, waiting for cardholder Acceptance

Step 2 - Waiting for Validation

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.19 - Waiting for Validation

Step 3 - Validation completed, Transaction approved

	12345678901234567890	
Line 1:	BUY: 123456,78 EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:	Approved	MC = '03'
Line 4:		

Figure 1-11.20 - Validation completed, Transaction approved

1-11.4 Display flow for Transactions - max. 16 Characters per Line

This section shows how the guiding text messages may be set up on the User Interface Display.

The use of the User Interface Display is shown by means of a number of transaction examples.

It is assumed that the User Interface Display used, is able to display at least 4 lines of each 16 characters only.

1-11.4.1 Example 1: Display flow PIN Trans. - Approved

This example is based on 'Combined PIN Entry and Amount Confirmation'.

Step 1 - PIN Entry Enabled but Amount not available yet

	1234567890123456	
Line 1:		
Line 2:		
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN	MC = '09'

Figure 1-11.21 - PIN entry enabled but Amount not available yet

Step 2 - PIN Entry Enabled and Amount available

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN/Accept	MC = 'EC'

Figure 1-11.22 - PIN entry enabled and amount available

Step 3 - PIN Entry completed and Amount accepted, waiting for Validation

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	
Line 4:	Please Wait	MC = '0E'

Figure 1-11.23 - PIN entry completed and Amount accepted, waiting for Validation

Step 4 - Validation completed, Transaction approved

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Approved	MC = '03'

Figure 1-11.24 - Validation completed, Transaction approved

1-11.4.2 Example 2: Display flow PIN Trans. - PIN Error

This example is based on 'Combined PIN Entry and Amount Confirmation'.

Step 1 - PIN Entry Enabled but Amount not available yet

	1234567890123456	
Line 1:		
Line 2:		
Line 3:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN	MC = '09'

Figure 1-11.25 - PIN entry enabled but Amount not available yet

Step 2 - PIN Entry Enabled and Amount available

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN/Accept	MC = 'EC'

Figure 1-11.26 - PIN entry enabled and amount available

Step 3 - PIN Entry Completed and Amount Accepted, Waiting for Validation

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Please Wait	MC = '0E'

Figure 1-11.27 - PIN entry completed and Amount accepted, waiting for Validation

Step 4 - Validation completed, Transaction rejected - PIN Error

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	Declined	MC = '07'
Line 4:	Incorrect PIN	MC = '0A'

Figure 1-11.28 - Validation completed, Transaction rejected - PIN Error

1-11.4.3 Example 3: Display flow PIN Trans. - PIN Retry

This example is based on 'Combined PIN Entry and Amount Confirmation'.

Step 1 - PIN Entry Enabled but Amount not available yet

	1234567890123456	
Line 1:		
Line 2:		
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN	MC = '09'

Figure 1-11.29 - PIN entry enabled but Amount not available yet

Step 2 - PIN Entry Enabled and Amount available

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN/Accept	MC = 'EC'

Figure 1-11.30 - PIN entry enabled and Amount available

Step 3 - PIN Entry completed and Amount accepted, waiting for Validation

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Please Wait	MC = '0E'

Figure 1-11.31 - PIN entry completed and Amount accepted, waiting for Validation

Step 4 - Validation completed, Transaction rejected - PIN Error (Texts are displayed for 6 seconds)

NOTE: This step may be skipped.

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	Declined	MC = '07'
Line 4:	Incorrect PIN	MC = '0A'

Figure 1-11.32 - Validation completed, Transaction rejected - PIN Error

Step 5 - Validation completed, Transaction rejected - PIN Error - (Remaining PIN attempts available - PIN Retry)

NOTE: If the number of PIN tries left is not displayed, line 3 may remain blank or the remaining information may be rearranged.

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	X PIN tries left	MC = 'F8', (X) indicates the number of PIN tries left
Line 4a:	Incorrect PIN	MC = '0A', alternating between line 4a and 4b
Line 4b:	Enter PIN/Accept	MC = 'EC', alternating between line 4a and 4b

Figure 1-11.33 - Validation completed, Transaction rejected - PIN Error - (Remaining PIN attempts available - PIN Retry)

Step 6 - When the Cardholder enters the first PIN Digit

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *	MC = 'EF' + an "*" for each digit entered
Line 4:	Enter PIN/Accept	MC = 'EC'

Figure 1-11.34 - When the cardholder enters the first PIN Digit

Step 7 - PIN Entry completed and Amount accepted, waiting for Validation

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Please Wait	MC = '0E'

Figure 1-11.35 - PIN Entry completed and Amount accepted, waiting for Validation

and so on.....

1-11.4.4 Example 4: Display flow Signature Trans. - Approved

This example is based on 'No Amount Acceptance'.

Step 1 - Amount available, waiting for Validation

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.36 - Amount available, waiting for Validation

Step 2 - Validation completed, Transaction approved

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Approved	MC = '03'

Figure 1-11.37 - Validation completed, Transaction approved

1-11.4.5 Example 5: Display flow Signature Trans. - Approved

This example is based on 'Amount Acceptance'.

Step 1 - Amount available, waiting for Cardholder acceptance

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Accept?	MC = 'F1'

Figure 1-11.38 - Amount available, waiting for cardholder acceptance

Step 2 - Waiting for Validation

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Please Wait	MC = '0E'

Figure 1-11.39 - Waiting for Validation

Step 3 - Validation completed, Transaction approved

	1234567890123456	
Line 1:	BUY: EUR	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Approved	MC = '03'

Figure 1-11.40 - Validation completed, Transaction approved

1-11.5 PIN Entry flow

1-11.5.1 Requirements for PIN Entry State

PIN entry shall only be possible when the Secure Device (SD), which includes the PIN Pad, is in the PIN Entry State.

The PIN Entry State is initiated when the Secure Device receives an *Initiate PIN Entry* command.

The *Initiate PIN Entry* command is defined in ref. 27: "TAPA, Application Architecture Specification".

The font and position of the messages shown in the figures below are only to be seen as examples.

- 1-11.5.1.1 A If the data element 'Number of PIN entries left' (defined in the *Initiate PIN Entry* command) indicates the number of tries left, then the Message Code 'F8' ("(x) PIN tries left") shall be displayed while PIN entry is enabled.

NOTE: (x) indicates the number PIN tries left. The examples given are in English and the Business Call 'Purchase' is used as default.

(X) PIN tries left

- 1-11.5.1.2 A If the most significant bit in the data element 'Number of PIN entries left' is set to 1, the Message Code '0A' ("Incorrect PIN") shall be displayed until the cardholder enters the first digit.

NOTE: If the most significant bit is set to 0, the Message Code '0A' shall *not* be displayed.

(X) PIN tries left
Incorrect PIN

- 1-11.5.1.3 A When PIN entry state is initiated by the *Initiate PIN Entry* command the Message Code '09' ("Enter PIN"), Message Code 'EF' ("PIN:") and an "*" for each PIN digit entered shall be displayed on the Cardholder Display.

PIN:
(X) PIN tries left
Incorrect PIN
Enter PIN

- 1-11.5.1.4 A When the PIN Entry State is initiated by the *Initiate PIN Entry* command, the Accept key shall remain inactive until either the *Get PIN* or the *Confirm Amount* command is received.

- 1-11.5.1.5 A When the Confirm Amount commands is received a corresponding text derived from the Business Call ("Buy"), the Amount and the Currency Code (in alpha-characters) shall be displayed on the Cardholder Display.

BUY: 123456,78 EUR
PIN: **
(X) PIN tries left
Enter PIN

- 1-11.5.1.6 A When either the *Get PIN* or the *Confirm Amount* command is received and the number of PIN digits match the Minimum PIN digits defined in the *Initiate PIN Entry* command, the Message Code '09' ("Enter PIN") shall be replaced by Message Code 'EC' ("Enter PIN and Accept").

```
BUY: 123456,78 EUR
PIN: ****
(X) PIN tries left
Enter PIN and Accept
```

NOTE: The order of events (command received vs. match of PIN digits) is not significant, but both conditions shall be fulfilled before the text is replaced.

- 1-11.5.1.7 A When the *Terminate PIN Entry* command is received the Message Code 'EC' ("Enter PIN and Accept") shall be replaced by Message Code '0E' ("Please Wait").

```
BUY: 123456,78 DKK
PIN: ****

Please Wait
```

- 1-11.5.1.8 C If the Cardholder Display is not able to display all the Message Codes simultaneously:
'F0' ("Buy:") with Amount and Currency Code
'F8' ("(x) PIN tries left"),
'0A' ("Incorrect PIN"),
'EF' ("PIN:") and
'09' ("Enter PIN")
the Message Codes '0A' and '09' may alternate until the first PIN digit has been entered.

1-11.6 Terms - Business Calls and Admin. Functions

1-11.6.1 Introduction

This section provides a translation of the Business Calls and Administrative Functions from English into Danish terms.

1-11.6.2 Business Calls

The following Business Calls are defined in the OTRS specification:

- Purchase
- Refund
- Original Authorization
- Supplementary Authorization
- Reversal (Authorization)
- Capture
- Cancellation
- Extended Authorization
- Top Up
- Post Purchase
- Post Refund

In addition, the following 'service functions' are defined:

- Gratuity or Extra
- Cashback

Based on the names used for similar functions on previous terminal implementations table 1-11.2 defines the names in English. Names in other languages can be found in the Regional Requirements, chapter 1-15.

Table 1-11.2 - Business Calls and Service Functions, texts

Function or Buss. Call	English (20 characters)	English (16 characters)
Purchase	Purchase or Buy *	Purchase or Buy*
Refund	Refund	Refund
Original/Extended Authorization	Authorization	Authorization
Supplementary Authorization	Suppl. Authorization	Suppl. Author.
Reversal (Authorization)	Reverse Authoriz.	Reverse Author.
Capture	Capture	Capture
Cancellation	Cancellation	Cancellation
Top Up	Top Up	Top Up
Gratuity or Extra	Extra	Extra
Cashback	Cashback	Cashback
Post Purchase	Post Purchase	Post Purchase
Post Refund	Post Refund	Post Refund
Legend: * = The most suitable name may be selected.		

1-11.6.3 Administrative Functions

According to the OTRS specifications, the terminal must support a number of Administrative Functions:

- Installation
- Advice Transfer
- Clock Synchronization
- PSAM Update Transfer
- PSAM Deactivate

Based on the names used for similar functions on previous terminal implementations table 1-11.3 defines the names in English.

Table 1-11.3 - Administrative Functions, text

Administrative Function	English
Installation	Installation
Advice Transfer	Advice Transfer
Clock Synchronization	Clock Synchron.
PSAM Update Transfer	PSAM Upd. Trans.
PSAM Deactivate	PSAM Deactivate
Legend: * = The most suitable name may be selected.	

1-12 Receipts

This section defines how and when receipts are to be printed.

The requirements are initially divided between the functional requirements for the generation of receipts and the requirements for the layout of the receipts.

The functional requirements starts with the generic requirements followed by the requirements for special environments like Unattended Payment Terminals.

The layout of the receipts is initially specified in a generic way, using English as default language, followed by a section with the additional requirements for DCC receipts. Information on the regional receipt requirements can be found in chapter 1-15 page 1-15-1, Regional Requirements.

The chapter holds generic as well as optional requirements. Whether or not the optional requirements shall be fulfilled depends on the application and the region of use. The regional requirements are specified in the individual sections in chapter 1-15.

1-12.1 Functional requirements

1-12.1.1 Generic

- 1-12.1.1.1 A A cardholder receipt shall as minimum be printed in the following cases:
- The transaction is successful,
 - A receipt is to be signed by the cardholder,
 - The cardholder has pressed the Enter button,
 - The terminal cannot determine, whether or not the cardholder has pressed the Enter button.

NOTE: For an OTRS terminal, this presuppose that the *Initiate Payment* command has been issued.

- 1-12.1.1.2 A Requirement 1-12.1.1.1 does not apply, i.e. a receipt shall not be printed, if one of the following conditions are met:
- The cardholder has chosen not to have a receipt,
 - There is a printing error during the transaction, the cardholder is informed about this, and decides to proceed without receipt printing,
 - The transaction is terminated due to fallback from ICC to MSC. For an OTRS terminal this is shown by an ASW1-ASW2 returned in the response to *Initiate Payment* command of the value '1222' or '1400'.

NOTE: It is allowed to start a transaction where a receipt cannot be printed, if the cardholder has been informed about this in advance, and has decided to proceed anyway.

- 1-12.1.1.3 A Requirement 1-12.1.1.1 may not apply, i.e. a receipt need not to be printed if the transaction meets the criteria for the “easy” or “quick” payment services from the card schemes.
- NOTE:** See information from the different card schemes regarding meeting the specific criteria.
- 1-12.1.1.4 A A “easy” or “quick” service terminal shall still be able to provide a receipt if the cardholder requests one.
- 1-12.1.1.5 A If the terminal is attended, the merchant shall be able to request a copy of the receipt from the previous transaction. If the previous transaction generated both a cardholder and a merchant receipt, both copies shall be printed.
- 1-12.1.1.6 A If signature forms part of the CVM selected, the receipt to be signed by the cardholder shall be printed after the card has been validated.
- This is, for an OTRS terminal, after the response to *Validate Data* command is known, but before the *Complete Payment* command is issued to the PSAM.
- 1-12.1.1.7 A The results from the signature validation shall be included in the processing, before the cardholder's receipt is printed. In this way, the merchant can stop/cancel the transaction.
- NOTE:** Some system may have the capability to be set to unconditionally accept the signature.
- 1-12.1.1.8 A For an OTRS terminal, the result from signature validation shall be included in the *Complete Payment* command.
- Technical problems during processing of the *Complete Payment* command may also cause the transaction to fail. Consequently, the final transaction result is not known until the response to *Complete Payment* has been received by the terminal.
- 1-12.1.1.9 A For an OTRS terminal, the cardholder's receipt indicating a successful result shall not be printed until the response to the *Complete Payment* command has been received from the PSAM.
- 1-12.1.1.10 A For an OTRS terminal, the cardholder's receipt indicating a not successful transaction shall be based on the first response from the PSAM indicating a non-approved result.
- 1-12.1.1.11 A An attended terminal shall be able to generate a merchant's receipt if it performs a offline transaction.
- 1-12.1.1.12 C It may be possible to enable and disable the generation of offline merchant receipts.
- 1-12.1.1.13 A If the merchant or the cardholder stops a transaction in progress before the cardholder has accepted the transaction by entering the PIN, the transaction shall be stopped/cancelled and the Transaction Information block part B, see figure 1-12.7 page 1-12-14, shall be omitted from the receipt and a Footer Information block, see figure 1-12.10 page 1-12-24, shall be added.

- 1-12.1.1.14 A If the merchant or cardholder is able to stop a transaction in progress *after* the cardholder accepted the transaction by entering the PIN, the transaction shall be stopped/cancelled and the Transaction Information block part B, see figure 1-12.7 page 1-12-14, shall be omitted from the receipt and a Footer Information block, see figure 1-12.10 page 1-12-24, shall be added to the receipt.
- 1-12.1.1.15 A If a transaction is declined, either by the host as response to an online request, locally by the ICC or after local validation (e.g. Stop List check) then a Footer Information block, see figure 1-12.10 page 1-12-24 shall be added to the receipt.
- 1-12.1.1.16 A If the signature is not accepted by the Attendant, then a Footer Information block shall be added to the cardholder's receipt indicating that the signature was rejected.
- 1-12.1.1.17 C For a signature transaction, if the cardholder is no longer present, when the final receipt adding gratuity is to be printed, the printing may be omitted.
- 1-12.1.1.18 A To be able to omit printing, the merchant shall, actively choose to skip the printing, for each individual transaction.
NOTE: Skipping the printing of a receipt shall not affect the capability of logging transaction data.
- 1-12.1.1.19 A If a transactions fails, either due to communication errors on the host link, or due to technical problems internally in the terminal (e.g. communication between the ICC and the Card Reader) then a Footer Information block shall be added to the receipt.
- 1-12.1.1.20 A In case of print failure e.g. paper jam, it shall be possible to get/print a copy of the receipt in an attended terminal irrespective of the transaction result.
- 1-12.1.1.21 C When generating a copy of the merchants receipt, the terminal may truncate the PAN to avoid that additional PCI-DSS requirements are inflicted on the solution. See section 1-7.1.3.
- 1-12.1.1.22 B The terminal/prINTER shall support the characters defined in ref. 12: "ISO/IEC 8859-15".

1-12.1.2 Special Considerations for Unattended Terminals

The fact, that no merchant is able to supervise the printing of receipts, introduces some specific requirements to unattended terminals (Unattended Payment Terminals). These requirements are changes or extensions to the generic requirements.

- 1-12.1.2.1 A For an unattended terminal, the cardholder shall be able to select whether or not a receipt is to be printed.
NOTE: Depending on the environment, the cardholder may be asked during the dialogue.
- 1-12.1.2.2 A For an unattended terminal the default shall be *not* to print a receipt.
NOTE: For some terminals, like ticket vending machines, the receipt may be the actual goods delivered. For these terminals the receipt is mandatory.

- 1-12.1.2.3 C For an unattended terminal, it may, for a limited time, be possible to get a copy of a previously printed receipt.
- 1-12.1.2.4 A For an unattended terminal, the cardholder shall, prior to starting a transaction, be informed if no receipt can be printed.
- 1-12.1.2.5 A For an unattended terminal, where a receipt cannot be printed, the cardholder shall be given the opportunity to proceed, knowing that no receipt can be printed.
- 1-12.1.2.6 B For an unattended terminal, the cardholder should be able to request a receipt if the transaction is declined, independent of his choice earlier in the transaction.
- An unattended terminal, where the payment sequence is Token based has special requirements with respect to receipt printing.
- If the exact amount is not known at the time of authorization e.g. self service petrol terminals, the Business Call Original/Extended Authorization may be used to initiate a payment sequence.
- Even if the exact amount is known at the time of authorization, the Business Call Original/Extended Authorization may be used to initiate a payment sequence. In this case the amount is shown to the cardholder for acceptance during the Original/Extended Authorization. If the delivery of the selected goods is awaiting the result of the Original/Extended Authorization, the Capture may be initiated after a successful delivery of goods. This procedure may be relevant for e.g. ticket vending machines.
- For an unattended terminal, where the payment sequence is Token based, the following applies;
- 1-12.1.2.7 A If the transaction sequence is interrupted/cancelled before the Capture is completed, then the printout of receipt(s) shall include a receipt for the Reversal (Authorization) performed, and for all rejected or failed authorization attempts, related to the actual sales flow.
- 1-12.1.2.8 A If the amount is *not* shown to the cardholder and the Capture is completed before printout of a receipt is requested/initiated then only the receipts derived from the Capture(s) shall be printed.
- 1-12.1.2.9 A If the amount *is* shown to the cardholder and the Capture is completed before printout of a receipt is requested/initiated, then receipts from any un-successful Original/Extended Authorizations as well as from the Capture(s) shall be printed

1-12.1.3 Automated Fuel Dispensers

The procedure to get a receipt in an unattended terminal depends on the actual implementation and the environment in which the terminal is installed.

In certain environments, e.g. automated fuel dispensers, the transaction processing is split into four steps :

- Pre-Authorization using the physical card and a default or pre-specified transaction amount,

- Delivery of goods and services, e.g. petrol,
- Capture performed automatically by the terminal when the final transaction amount is known,
- Receipt printing.

1-12.1.3.1 A Single-user terminals shall fulfil requirement 1-12.1.3.2, whereas multi-user terminals shall fulfil requirements 1-12.1.3.3 to 1-12.1.3.5.

Single-user Automated Fuel Dispenser

1-12.1.3.2 A If access to the user interface is dedicated to a single cardholder throughout the entire transaction, the decision whether a receipt shall be printed or not shall be taken via cardholder dialogue.

Multi-user Automated Fuel Dispenser

1-12.1.3.3 C If access to the user interface is shared with other cardholders throughout the entire transaction, the decision on whether or not a receipt shall be printed, should be taken via a cardholder dialogue during the pre-Authorization part of the transaction.

1-12.1.3.4 A If the cardholder returns to the terminal after delivery of goods and services, the cardholder shall be able to select printout of the receipt.

1-12.1.3.5 C If the user interface is shared with other cardholders, the receipt may be selected by a payment reference based on the PAN of the card, i.e. by the user re-inserting the card.

All Automated Fuel Dispenser

1-12.1.3.6 A If the selection of the receipt is based on information including the PAN, the implementation shall fulfil the PCI-DSS requirements with respect to storage of PAN and derived information.

1-12.1.3.7 A If the selection of receipt is based on re-inserting the card into the terminal, the design shall ensure, that the cardholder doesn't enter his PIN unintentionally.

NOTE: The terminal could for instance check that no receipts related to a specific PAN, are stored in the terminals, before a transaction is started.

1-12.1.3.8 B It shall *not* be possible for a cardholder to print out the receipt from a preceding cardholder.

NOTE: If the preceding cardholder has decided to get a receipt but did not return to have it printed, it may be possible for anybody to have it printed, e.g. for a limited period.

1-12.1.4 DCC Functional Requirement

- 1-12.1.4.1 A A terminal supporting DCC, and not performing on-display currency selection, shall be able to print a pre-receipt.

- 1-12.1.4.2 A It shall not be possible to select DCC, if the terminal don't support on-display currency selection and a pre-receipt cannot be printed.

1-12.2 Standard Receipt Layout

This section defines the layout of receipts. The layout is defined in two steps. There is initially a definition of a generic receipt layout. This is followed by sections specifying definitions for special receipt types/environments; this is e.g. the case with receipts for Dynamic Currency Conversion transactions. All layouts shown in this section are based on a receipt printer able to print 24 characters per line.

1-12.2.1 Receipt Language

The reference language used is English. Information on the layout to use for other languages, including Danish, can be found in section 1-15.2 and forward. With respect to selecting receipt print languages the following generic rules apply;

- | | | |
|------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-12.2.1.1 | A | The default language to use shall be the (merchant) local language. |
| 1-12.2.1.2 | A | The terminal shall as well be able to use English as the receipt language. |
| 1-12.2.1.3 | A | The terminal shall support language selection according to reference 20 "EMV ICC Specification", chapter 11. |
| 1-12.2.1.4 | A | If the card is an ICC and the card has a preferred language and the terminal supports this language, then the terminal shall initially select this language as the preferred language to be used on the receipt. |
| | | NOTE: Support of a language shall be interpreted as being able to use the texts as defined in section 1-15, i.e. languages not listed in this section shall be interpreted as not supported. |
| 1-12.2.1.5 | C | The terminal may have a capability for manually selecting the language to be used on the receipt. |
| 1-12.2.1.6 | C | If another language than the local language has been chosen for the Cardholders display on terminal, then this language should be used for the Cardholders receipts as well. |
| 1-12.2.1.7 | C | If the language on the Cardholders display is changed, then the language on the Cardholders receipt may follow. |
| 1-12.2.1.8 | A | Localization of the receipt texts shall be implemented using the text definitions in section 1-15. |
| 1-12.2.1.9 | B | The terminal/printer shall support the character set defined in ref. 12: "ISO/IEC 8859-15". |

Specific requirements for DCC are listed in section 1-12.3 page 1-12-27, DCC Receipt Layout.

1-12.2.2 Emphasizing of Text

Parts of the text on the receipts are emphasized to make it stand out. This is the case for header information, footer information and the total amount.

The default way of emphasizing header and footer information is by enclosing the information within lines of 'stars', "*****". Examples of this are the lines HI1, HI6 and FI3 in the receipt layout.

- 1-12.2.2.1 C The header information and the footer information may be emphasized in one or more of the following ways (may be combined).

Using a bold font, where the stroke is at least 30% heavier than the stroke of the surrounding text.

Using a larger font, where the size of the font is at least 25% larger than the font of the surrounding text.

*****	Default
COPY	Default
*****	Default
COPY	Large font
COPY	Bold text

Figure 1-12.1 - Header empathizing

The default way of emphasizing the amount is by enclosing the line with lines of 'dashes' - "-----".

- 1-12.2.2.2 C The total amount information may as well be emphasized in the following way;

- Using a bold font and at the same time underlining the amount.
- Using a large font and at the same time underlining the amount.

TOTAL	EUR	139200,00	Default
			Default
TOTAL	EUR	<u>139200,00</u>	Bold & underline
TOTAL	EUR	<u>139200,00</u>	Large & underline

Figure 1-12.2 - Amount empathizing

1-12.2.3 Generic Layout

The specification of the layout divides the generic structure of a receipt into a number of blocks. Not all of these blocks are mandatory for all receipts. The blocks are;

- Receipt Header
- Merchant Information
- Header Information
- Amount Information
- Transaction Information
- Signature Information
- Footer Information
- Prepaid Card Information
- Receipt Footer

The lines within a block are numbered for reference. Not all lines within a block are mandatory, and some lines may be

mutually exclusive. Each line may sometimes be split into two or more fields holding different information.

The blocks are defined in the following sections. There is for each block, a figure showing the possible lines within the block.

- 1-12.2.3.1 A A receipt shall at least consist of the following blocks;
- Merchant Information
 - Header Information
 - Amount Information
 - Transaction Information
- 1-12.2.3.2 A A pre-receipt shall at least consist of the following blocks.
- Merchant Information
 - Information Header
 - Amount Information
- 1-12.2.3.3 A If a receipt is to be printed and not all of the information is available yet, then the field(s) not available shall as default be filled with space(s).

A generic receipt, with all of the lines for the information blocks is shown in figure 1-12.4.1 page 1-12-44.

1-12.2.4 Quick Receipt

- 1-12.2.4.1 C Transactions meeting the criteria for “quick” or “easy” transaction services from the card schemes may qualify for a reduced receipt format.
- 1-12.2.4.2 A The reduced receipt format requires the following information on the receipt;
- The merchants name,
 - The total transaction amount,
 - The transaction date,
 - The truncated account number **or** confirmation that the cardholder paid using the <Card Product name>.
- NOTE:** There is no detailed specifications for the format of the receipt data.

1-12.2.5 Receipt Header

- 1-12.2.5.1 C A receipt and a pre-receipt may contain a Receipt Header block. The receipt header may contain information such as merchant logo, clerk identification, checkout identification and specification of services. The structure of this block is outside the scope of this document.

1-12.2.6 Merchant Information

- 1-12.2.6.1 A The format of the Merchant Information block shall be as shown in figure 1-12.3 page 1-12-10.
- 1-12.2.6.2 A For an OTRS terminal, the variable information printed shall be retrieved from the *Exchange Debit/Credit Static Information* command.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5

Figure 1-12.3 - Merchant Information block

- 1-12.2.6.3 A A receipt shall, if the information is not preprinted on the receipt, have a line MI1 holding the name of the merchant.
This information is, for an OTRS terminal, available in the data element "ME_{NAME}".
- 1-12.2.6.4 A A receipt shall, if the information is not preprinted on the receipt, have a line MI2 holding the address of the merchant.
This information is, for an OTRS terminal, available in the data element "ME_{ADDRESS}".
- 1-12.2.6.5 A A receipt shall, if the information is not preprinted on the receipt, have a line MI3 holding the zip-code and the city name of the merchant.
This information is, for an OTRS terminal, available in the data elements "ME_{ZIP}" and "ME_{CITY}".
- 1-12.2.6.6 C A receipt should, if the information is not preprinted on the receipt, have a line MI4 holding the "Phone number". The line shall, if present, contain a header of "Phone:" followed by the data element "Merchant Phone".
This information is, in an OTRS terminal available in the data element "ME_{PHONE}". The header shall be printed in the chosen language.
- 1-12.2.6.7 A A receipt shall, if the information is not preprinted on the receipt, have a MI5 line holding the "Bus. reg. number". The line shall have a header of "BUS.REG.NO:" followed by the data element "Business Registration Number".
This information is, for an OTRS terminal, available in the data element "ME_{BRN}". The header shall be printed in the chosen language.

1-12.2.7 Header Information

- 1-12.2.7.1 A The format of the Header Information block shall be as shown in figure 1-12.4.

*****	HI1
COPY	HI2
*****	HI3
PRELIMINARY	HI4
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10

Figure 1-12.4 - Header Information Block

- 1-12.2.7.2 A A receipt shall, if it is a copy of a previously printed receipt, have the lines HI1, HI2 and HI3. Line HI2, "Copy indicator" shall be translated to the chosen language.
- NOTE:** The emphasizing of the text may be achieved in other ways, see section 1-12.2.2 page 1-12-7, Emphasizing of text.
- 1-12.2.7.3 A A receipt shall, if it has line H4 or HI5, have line HI3 and HI6 as well. Line HI4, "Prelim/post indicator" and line HI5 "Non-financial indicator" shall be translated to the chosen language.
- 1-12.2.7.4 A Line HI4 "Prelim/post indicator" shall be present if it is a pre-receipt. The text shall be "PRELIMINARY". The text shall be translated to the chosen language.
- 1-12.2.7.5 A Line HI 4 "Prelim/post indicator" shall be present if the receipt is the documentation of a manual key entry of a previous non-electronic transaction (post registration). The text shall be "POST REGISTRATION". The text shall be translated to the chosen language.
- NOTE:** Such a transaction may be necessary if there has been a breakdown of the terminal or the network.
- 1-12.2.7.6 A A receipt shall, if it is the documentation of a cancellation have line HI4 "Cancellation indicator" with the text "CANCELLATION".
- 1-12.2.7.7 A Line HI5 "Non-financial indicator" shall be present if it is a pre-receipt, or if the transaction documented by the receipt is an Authorization or the Reversal of an Authorization.
- 1-12.2.7.8 A A receipt shall, if it isn't the documentation of a purchase of goods and services, have the lines HI6, HI7, and HI8. The content of line HI7, "Trans. indicator" shall be according to table 1-12.1. The line shall be translated for terminals using other languages. See note at requirement 1-12.2.7.2 page 1-12-11 with respect to emphasizing.

Table 1-12.1 - Transaction and related Header Text

Transaction	Header text
Purchase	No header text
Manual Cash Disbursement	CASH
Authorization	AUTHORIZATION ONLY
Refund	REFUND
Cancellation	<as cancelled transaction>
Reversal of Authorization	REVERSAL (AUTH.)

- 1-12.2.7.9 B A receipt should, for formatting purposes, have a HI9 line.
- 1-12.2.7.10 A A receipt shall have line HI10 holding the date and time. The date shall be left-justified and have the format YYYY-MM-DD. The time shall be right-justified and have the format hh:mm.
- 1-12.2.7.11 A The data and time printed on the receipt shall be the same as the date and time for the corresponding transaction.
- NOTE:** The date and time for a capture, shall be the time of the capture and not the time of the Authorization.

- 1-12.2.7.12 A If a copy of a previous receipt is printed, the date and time shall be the same as on the original receipt.
- 1-12.2.7.13 C A receipt may use an extended time format of hh:mm:ss.

1-12.2.8 Amount Information

- 1-12.2.8.1 A The format of the Amount Information block shall be as shown in figure 1-12.5 page 1-12-12.
- 1-12.2.8.2 C Certain special setups, like the use of DCC, may have two Amount Information blocks on a single receipt.

AMOUNT	EUR	123456,78	AM1
		-----	AM2
			AM3
VAT INCL.	EUR	12345,67	AM4
SURCHARGE	EUR	2345,67	AM5
CASHBACK	EUR	1000,00	AM6
EXTRA	EUR	51,88	AM7
		-----	AM8
TOTAL	EUR	139200,00	AM9
		-----	AM10
EXTRA	EUR		AM11
		-----	AM12
TOTAL	EUR		AM13
		-----	AM14
			AM15

Figure 1-12.5 - Amount Information block

- 1-12.2.8.3 C A receipt should, for formatting purposes, have a AM1 line.
- 1-12.2.8.4 A A receipt shall have a line AM2, "Amount type". The header text, in the example "AMOUNT" shall be according to table 1-12.2. The header text shall be translated to the chosen language.

Table 1-12.2 - Business Calls and related Header Text

Business Call	Header text
Purchase	PURCHASE
Refund	RETURN
Cash	CASH
Others (Capture, Authorization etc.)	AMOUNT

- 1-12.2.8.5 A The Alphabetic Currency Code (e.g. "EUR") shall for lines AM2 through AM9 and AM11 be as follows;
 - for non-DCC transactions it shall be the currency code for the currency selected for the transaction.
 - for DCC transactions it shall be the merchant's (local) currency code in the first block and the cardholder's billing currency code in the second block.

NOTE: The currency code is, for an OTRS terminal, available in the data element "CURRC". The default cur-

rency code is the merchants local currency, but the terminal may support multiple currencies.

- 1-12.2.8.6 A The amount shall, for a Purchase or Capture transaction be the final amount i.e. the amount that will be transferred to the merchant's account. For a Purchase with gratuity it shall be the amount for goods and services before gratuity is added.
- 1-12.2.8.7 A The amount shall, for a Refund transaction be the final amount i.e. the amount that will be transferred to the cardholder's account.
- 1-12.2.8.8 A The amount shall, for an Authorization, be the amount authorized.
- 1-12.2.8.9 B The amount shall, for an Authorization, be omitted if the value is not relevant to the cardholder.
- NOTE:** In some environments, e.g. self service petrol terminals, the amount authorized may have no importance and may even be confusing to the cardholder. This is as well the case for the balance inquiry on a Prepaid MSC.
- 1-12.2.8.10 A A receipt shall, if Value Added Tax, VAT, line AM4 is to be printed, but no total is printed, have a line AM3 to emphasize the amount.
- 1-12.2.8.11 C The emphasizing may as well be achieved in other ways, see section 1-12.2.2.
- 1-12.2.8.12 B A receipt shall have the line AM4, if VAT is to be printed on the receipt. The header text for line AM4 shall be "VAT.INCL". The header text shall be translated to the chosen language.
- 1-12.2.8.13 B A receipt shall, if surcharge is to be paid by the cardholder, and surcharge is to be printed, have a line AM5. The header text shall be "SURCHARGE". The header text shall be translated to the chosen language.
- 1-12.2.8.14 B A receipt shall, if surcharge is to be paid by the cardholder and surcharge is not stated explicit, have a line AM5. The text shall be "INCLUDING SURCHARGE". The header text shall be translated to the chosen language.
- 1-12.2.8.15 A A receipt shall, if "Amount Other" information is transferred to the host, have the line AM6. The header text shall be "CASHBACK". The header text shall be translated to the chosen language.
- 1-12.2.8.16 A A receipt shall, if tips or gratuity has been added to the amount for goods and services, have a line AM7. The header text shall be "EXTRA". The header text shall be translated to the chosen language.
- 1-12.2.8.17 A A receipt shall have the line AM9, if any of the lines AM5 through AM7 are present. The header text shall be "TOTAL". The header text shall be translated to the chosen language. The amount shall be the sum of the amounts in lines AM2, AM5, AM6 and AM7.

- 1-12.2.8.18 A A receipt shall, if line AM9 is present, have lines AM8 and AM10 for formatting purpose.
- NOTE:** The emphasizing of the text may be achieved in other ways, see 1-12.2.2 page 1-12-7, Emphasizing of text.
- 1-12.2.8.19 A A receipt shall not have a line AM11, if a line AM7 has already been printed.
- NOTE:** Tips or gratuity must only be added to the amount once.
- 1-12.2.8.20 A A receipt shall have a line AM11, if tips or gratuity can be added to the amount by the cardholder, after the receipt has been printed. The header text shall be "EXTRA". The header text shall be translated to the chosen language.
- 1-12.2.8.21 A A receipt shall have lines AM12 and AM13, if it has a line AM11. The header text shall be "TOTAL". The header text shall be translated to the chosen language.
- 1-12.2.8.22 A A receipt shall have a line AM14. If there is but a single amount, then the line may be emphasized in other ways, see section 1-12.2.2 page 1-12-7, Emphasizing of text.
- 1-12.2.8.23 C A receipt should, if the Amount block consists of AM2 and AM3, have a line AM15 for formatting purposes.

1-12.2.9 Transaction Information

- 1-12.2.9.1 A The Transaction Information block shall consist of two parts, part A and part B as shown in figure 1-12.6 and 1-12.7.
- The Transaction Information block will be divided by the Signature Information block if a signature based transaction is performed.

PIN USED	TR1
MASTERCARD GOLD PSN:00	TR2
CONTACTLESS	TR3
DEBIT TRANSACTION	TR4
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
ACQUIRER NAME	TR7
ACQUIRER MERCHANT NUMBER	TR7a
IB1 ME.NO: 1234567890	TR8

Figure 1-12.6 - Transaction Information block, part A

ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORISED	TR14

Figure 1-12.7 - Transaction Information block, part B

- 1-12.2.9.2 C A receipt may, in certain regions, have line TR1 if the transaction is a PIN transaction. The text "PIN USED" shall be left justified. The header text shall be translated to the chosen language.
- NOTE:** The same information can be obtained from the second character of the TCC in line TR8.
- 1-12.2.9.3 A Line TR1 shall be omitted if the transaction is not a PIN transaction.
- 1-12.2.9.4 A A receipt shall have a line TR2. The content of the line is the "Card Name" and optionally a "PAN Sequence Number".
- 1-12.2.9.5 A The "Card Name" shall always be printed. The source of the Card Name shall be (prioritized list);
1. The Application Label (Tag '50') from the ICC (if present).
 2. Data received in the response from the host (if a response is received).
 3. Response to the *Initiate Payment* command.
 4. Tables stored locally in the terminal. Can be obtained by the *Get Debit/Credit Properties* command (with Identifier = '0001'/'0009'/'0012').
- NOTE:** In an OTRS terminal, the data from host can be retrieved in the response to either an Authorization Request or a Financial Request.
- NOTE:** In an OTRS terminal the locally stored data can be retrieved in the response to the *Initiate EMV Payment*, the *Initiate MSC Payment* or the *Initiate Key Entered Payment*.
- 1-12.2.9.6 B For the "PAN Sequence Number" the header shall be "PSN:". The header and the PAN Sequence Number shall only be printed if it is an ICC transaction and a valid Pan Sequence Number is available from the ICC (Tag '5F34') or it is a MSC track3 transaction where the PSN is available from the mag-stripe. A valid value is a 2 digit decimal number.
- NOTE:** In an OTRS terminal, the information can be retrieved in the response to the *Initiate EMV Payment*, the *Initiate MSC Payment2* or *Initiate Token Based Payment*.
- 1-12.2.9.7 C A receipt may, in certain regions, have a line TR3 if the processing conditions for transaction has generated a Payment Condition. The text "PAYM.CODE:" shall be left justified. The header text shall be translated for terminals using other languages. The actual Payment condition shall be a 6 character alphanumerical field directly following the header text. The content of the field shall be internally right justified and padded with leading spaces.
- 1-12.2.9.8 A It is, for contactless transactions, required that this is clearly indicated on the receipt. Line TR3 shall for a contactless transaction contain the text "Contactless" or "<card scheme> Contactless". Information about the card scheme can be derived from the AID of the card.

-
- 1-12.2.9.9 A Line TR3 shall be omitted if the transaction is not a contact-less transaction or the processing conditions for the transaction does not generate a Payment Condition.
- 1-12.2.9.10 A Line TR4 shall be omitted if the transaction does not contain an Account Type Selection or the Account Type code is '00'.
- 1-12.2.9.11 C A receipt may, in certain regions, have a line TR4 if the card used supports Account Type Selection. The header text, "DEBIT TRANSACTION" in the example, shall be according to table 1-12.3. The text shall be left justified. The text shall be printed in the chosen language.

Table 1-12.3 - Account Type and Related Text

Account type code	Text
10	SAVINGS TRANSACTION
20	DEBIT TRANSACTION
30	CREDIT TRANSACTION

- 1-12.2.9.12 A A receipt shall have a line TR5. The content of the line is the PAN.
- 1-12.2.9.13 A The PAN shall be truncated too all but the last four digits, see table 1-12.4. The character capital "X" shall be printed as masking character. Truncation shall be made for all cards. The truncated PAN shall be left justified and printed in blocks of four digits.

Table 1-12.4 - Truncation vs. Number of Digits in the PAN

Number of digits	PAN	Truncated PAN
10	1234 5678 90	XXXX XX78 90
11	1234 5678 901	XXXX XXX8 901
12	1234 5678 9012	XXXX XXXX 9012
13	1234 5678 9012 3	XXXX XXXX X012 3
14	1234 5678 9012 34	XXXX XXXX XX12 34
15	1234 5678 9012 345	XXXX XXXX XXX2 345
16	1234 5678 9012 3456	XXXX XXXX XXXX 3456
17	1234 5678 9012 3456 7	XXXX XXXX XXXX X456 7
18	1234 5678 9012 3456 78	XXXX XXXX XXXX XX56 78
19	1234 5678 9012 3456 789	XXXX XXXX XXXX XXX6 789

- 1-12.2.9.14 A Truncation shall be made on all receipts and receipt copies handed over to the cardholder.
- 1-12.2.9.15 C Receipts kept by the merchant, e.g. receipts signed by the cardholder may be without truncation.
- 1-12.2.9.16 B A receipt with an non truncated PAN shall *not* be stored electronically as clear text.
- NOTE:** Storage of a merchants receipt with un-truncated PAN, in order to be able to generate a copy, will enforce PCI security requirements on the system.
- NOTE:** The storage of a paper receipt by the merchant may serve as a transaction backup in offline conditions, for PIN as well as Signature transactions.
- 1-12.2.9.17 A A receipt shall have a line TR6. The content of the line is a transaction identification. It consists of a fixed header text of "TERM:" followed by a "Terminal Identification" and the STAN.
- NOTE:** For an OTRS terminal, the STAN will normally be returned in the response to the *Initiate Payment* command.
- NOTE:** For an OTRS terminal, the STAN will as well be returned in the response to the *Validate2* command in case of PIN retry when using a MSC.

- 1-12.2.9.18 A The "Terminal Identification" shall be printed as 8 alphanumeric characters. The STAN shall be printed as 6 numerical characters with leading zeroes. The two fields shall be separated by a '-'.
- 1-12.2.9.19 B A receipt shall have two lines TR7 and TR7a. The contents of the lines shall be "Acquirer information" and "Acquirer Merchant Number". The text shall be left justified. See section 1-10.5.8 for further information.
- 1-12.2.9.20 A A receipt shall have a line TR8. The content of the line shall be the "Transaction Condition Code", TCC, and a "Merchant Number".
- 1-12.2.9.21 A The Transaction Condition Code shall consist of three characters indicating Card Data Entry, CVM and Authorization respectively, as specified in table 1-12.5 page 1-12-18.
- 1-12.2.9.22 C The TCC may be blank or partially blank if the transaction is not successful.

Table 1-12.5 - Transaction Condition Codes

Card Data Entry		CVM		Authorization	
Code	Description	Code	Description	Code	Description
D	Magnetic stripe Track2	@	Signature based	1	Online authorization
E	Magnetic stripe Track2 as fallback for ICC	A	Online PIN	3	Offline, amount < floor limit ¹⁾
I	ICC Contact	B	Offline PIN	4	(Referral)
K	ICC Contactless	C	No CVM	5	Refund (online/offline) or forced offline for other Business Calls ¹⁾
L	MSD Contactless	M	Mail order		
T	Key entered	P	Phone order		
		V	(Online PIN and signature based)		
		W	Offline PIN and signature based		
		F	On Device CVM / Consumer Device CVM		

Legend:

¹⁾ For an OTRS-terminal the code '3' shall be used if the transaction is performed offline and the Merchant Initiative does not indicate forced offline (i.e. B' X10X XXXX) Code '5' shall be used if the transaction is performed offline and the Merchant Initiative indicates forced offline (i.e. B' X11X XXXX).

The code indicating Card Data Entry may, for an OTRS terminal, be based upon the following data:

- the type of card technology (ICC, MSC and Key Entered)
- POS Entry Mode or CVM Status

The code indicating CVM may be based upon the following data:

- CVM Status

The code indicating Authorization may, for an OTRS terminal, be based upon the following data:

- CVM Status (from *Validate Data 2* response)
 - Business Call
 - Merchant Initiative
- 1-12.2.9.23 A The "Merchant number" shall consist of a header text of "ME.NO." followed by a number. The number shall be a string of 10 decimal digits padded with leading zeroes. The header text shall be printed in the chosen language.
- This information is, for an OTRS terminal, available in the data element "ME_{NUMBER}".
- 1-12.2.9.24 A Lines TR8 and TR9 shall be separated by the Signature Information block, if the transaction is a signature transaction.
- 1-12.2.9.25 A A receipt shall have a line TR9 only if the transaction is an ICC transaction or the Capture of an earlier ICC authorization. The content of the line is the "Application Transaction Counter" and the "Application Effective Date".
- 1-12.2.9.26 A The "Application Transaction Counter", ATC, shall consist of a header text of "ATC:" followed by a number. The number is available from the ICC (Tag '5F34') and shall be a string of 5 numerical characters padded with leading zeroes.
- NOTE:** The information is, for an OTRS terminal, returned in the response to the *EMV Payment* or optionally in the response to the *Token Based Payment* command. An ATC value of '0000' indicates that "ATC:" and the corresponding value should be omitted.
- 1-12.2.9.27 A The "Application Effective Date", AED, shall consist of a header text of "AED:" optionally followed by a number. The number is optionally available from the ICC (Tag '5F25'). The number shall, if it is a numeric value different from '000000' be printed as a string of 6 numerical characters.
- NOTE:** The information is, for a OTRS terminal, returned in the response to the *Initiate EMV Payment* or optionally in the response to the *Initiate Token Based Payment* command.
- 1-12.2.9.28 A A receipt shall have a line TR10 only if the transaction is an ICC transaction or the Capture of an earlier ICC authorization. The content of the line is the "Application Identifier", AID. It shall consist of a header text of "AID:" followed by a hexadecimal number. The number is available from the ICC (Tag '4F') and shall be a right justified string of up to 20 characters of hexadecimal information.
- 1-12.2.9.29 C A terminal may, if the AID exceeds 20 hexadecimal characters, print the information over two lines. Both strings shall be right justified.
- 1-12.2.9.30 A If the terminal is an OTRS terminal, a receipt shall have a line TR11. The text "PSAM:" shall be fixed. The seven least significant decimal digits of the data element "ID_{PSAMCREATOR}" concatenated with the data element "ID_{PSAM}" shall be printed as 7 + 10 decimal digits.

NOTE: Example:
 RID_{PSAM} = 'A0 00 00 01 20' (not part of print)
 ID_{PSAMCREATOR} = '81 11 00 02' (2165374978)
 ID_{PSAM} = '00 00 02 1C' (540)
 Line TR11 = "PSAM: 5374978-0000000540"

NOTE: The information is returned in the response to the *Start-up PSAM* command.

1-12.2.9.31 A A receipt shall have a line TR12. The content of the line is the "Authorization Response Code" and the "ActionCode".

1-12.2.9.32 A The "Authorization Response Code" shall only be present, if it is an ICC transaction. It shall consist of a header text of "ARC:" optionally followed by 2 alphanumerical characters. The characters shall be printed, if the response received is different from hexadecimal '0000'.

NOTE: The information is, for an OTRS terminal, returned in the response to the *Validate Data 2* command.

1-12.2.9.33 A The "Action Code" shall consist of a header text of "STATUS:" optionally followed by 4 alphanumerical characters. The header text shall be translated to the chosen language. The four characters shall be printed, if the transaction is an online transaction. The data shall be fetched from the response to the *Validate Data 2* command.

NOTE: The information is as well, returned in Field 39/Data Element 39 in the response from the host. Data should not be retrieved here.

1-12.2.9.34 A A receipt shall have a line TR13. The content of the line is the "Approval Code". The line shall consist of a header text of "AUTH CODE:" optionally followed by six alphanumerical characters, right justified. The header text shall be translated to the chosen language. The information from the Host is returned in the response to the *Validate Data 2* command. Manually entered data are returned in the response to the *Check Stop List* command. The field shall be blank if no data is available.

NOTE: The information is as well, returned in Field 39/Data Element 39 in the response from the host. Data should not be retrieved here.

1-12.2.9.35 A A receipt shall have a line TR14. The content of the line is the "Reference No." and the "Authorization Result".

1-12.2.9.36 A The "Reference No." shall consist of a header text of "REF:" followed by a Reference STAN. The header text shall be translated to the chosen language. The Reference STAN shall, for a token based transactions, be the STAN used during the authorization. It can be retrieved by calling *Get D/C Properties* with an Index of '000A' after the *Validate Data* command. A token based transaction can be identified by a Card Data Source of "Token" during the *Initiate Token Payment* command. The reference STAN shall, for all non-token transactions be the STAN returned in the response to *Initiate Payment* command. The STAN shall be printed as 6 numerical characters padded with leading zeroes.

- 1-12.2.9.37 A The "Authorization Result" consists of a right justified text string, up to 14 characters long. The text string shall be "AUTHORIZED", if the transaction is completed successfully, else the text string shall be blank. The text string shall printed in the chosen language.

1-12.2.10 Signature Information

- 1-12.2.10.1 A A receipt shall contain a Signature Information block if the cardholder (Signature purchase) or the Merchant (Refund) has to sign a receipt. A pre-receipt shall contain a Signature Information block (surcharge information) if the pre-receipt is generated before the payment card is known. The format of the Signature Information block shall be as shown in figure 1-12.8 page 1-12-21.

	SI1
** VID EKSTRA **	SI2
KOM IHÅG NYT KVITTO	SI3
** WHEN TIPPING **	SI4
ASK FOR NEW RECEIPT	SI5
APPROVED FOR CREDITING	SI6
OF ACCOUNT	SI7
PRINTED DIGITS:	SI8
IDENTIFICATION:	SI9
(PASSPORT ETC:)	SI10
	SI11
.....	SI12
JURISDICTION OF ISSUE:	SI13
	SI14
.....	SI15
ID EXPIRY DATE:	SI16
	SI17
CLERK ID:	SI18
A FEE OR A SETUP CHARGE	SI19
MAY BE ADDED TO THE	SI20
CARDHOLDER'S ACCOUNT BY	SI21
THE ISSUER	SI22
	SI23
	SI24
	SI25
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28

Figure 1-12.8 - Signature Information block

- 1-12.2.10.2 B A signature receipt should, for formatting purposes, have a SI1 line.

- 1-12.2.10.3 A A signature receipt shall, for receipts where fields AM9 through AM11 are present, have a "Tips Informative Message" in lines SI2 through SI3. The message shall be in the chosen language.

NOTE: This type of receipt is generated when gratuity/tips can be added by the cardholder after the receipt has been printed.

- 1-12.2.10.4 C A signature receipt may, for certain regions, have the "Tips Informative Message in English as well as in lines SI4 through SI5.

- 1-12.2.10.5 C A signature receipt, may for some regional versions have a "Approval message" in lines SI6 and SI7. The text shall be according to table 1-12.6. The text shall be translated to the chosen language.

Table 1-12.6 - Business Call and related Approval Text

Business Call	Text
Refund	APPROVED FOR CREDITING OF ACCOUNT
Other	APPROVED FOR DEBITING OF ACCOUNT

- 1-12.2.10.6 A A signature receipt, from a manual cash disbursement terminal, shall have lines SI8 through SI18.

- 1-12.2.10.7 C A signature receipt, may for some regional versions, contain "ID source", lines SI9 through SI12, or parts thereof. The text shall be translated to the chosen language.

- 1-12.2.10.8 A A signature receipt shall, for a manual cash disbursement, contain a "Jurisdiction of issue", lines SI13 - SI15. The text shall be translated to the chosen language.

- 1-12.2.10.9 A A signature receipt shall, for a manual cash disbursement, contain a "ID expiry date", line SI16. The text shall be translated to the chosen language.

- 1-12.2.10.10 A A signature receipt shall, for a manual cash disbursement, contain a "Clerk ID", lines SI17 through SI18.

- 1-12.2.10.11 C A signature receipt may, for some regional versions of a refund transactions, contain a "Clerk ID", lines SI17 through SI18. The text shall be translated to the chosen language. These may as well, for certain regions, be used for offline Signature transaction.

- 1-12.2.10.12 A A signature receipt or a pre-receipt shall, for some special receipts have a "Signature Informative message" in lines SI15 through SI25, or a sub-range thereof.

- 1-12.2.10.13 C On a manual cash disbursement transaction receipt, a "Cash fee info" message lines SI19 - SI22 may be added. The text shall be "A fee or setup charge may be added to the cardholder's account by the issuer".

- 1-12.2.10.14 A A pre-receipt issued before the card is known shall, if surcharges are charged on the cardholder, have a "Signature Informative message". It shall consist of lines SI15 through SI25 or a sub-range thereof. It shall have a message header followed by a table of fee entries. The message header shall read "**** Please notice ****" \ "Surcharge will be added if paying by card".

NOTE: The '\ ' in the text above indicates that the information shall continue on a new line.

NOTE: The lines SI15 through SI25 are used for other information in other receipt types.

**** PLEASE NOTICE ****	SI15
SURCHARGE WILL BE ADDED	SI16
IF PAYING BY CARD	SI17
AMERICAN EXPRESS: +4,56%	SI18
DINERS: +3,45%	SI19
JCB: +2,34%	SI20
MAESTRO: +1,23%	SI21
MASTERCARD: +2,34%	SI22
VISA: +2,34%	SI23
VISA ELECTRON: +2,34%	SI24
	SI25

Figure 1-12.9 - Signature informative message, pre-receipt.

NOTE: The "Signature Informative message" will never be applicable to DCC (pre)-receipts, as a DCC pre-receipt cannot be issued before the PAN is known.

- 1-12.2.10.15 A The fee entries shall read "<Card scheme>: <fee percentage>". All supported card schemes and corresponding surcharge rates shall be printed. Card schemes not supported by the actual merchant shall not be printed. Surcharge rates printed shall be the rates actually paid by the merchant. An example is shown in figure 1-12.9 page 1-12-23.
- 1-12.2.10.16 A A signature receipt shall have the lines SI26 through SI28. The text in line SI26, "Signatory identifier" shall be according to table 1-12.7. The text shall be translated to the chosen language.

Table 1-12.7 - Business Call and related Signatory Text

Business Call, etc.	Signatory text
Refund	MERCHANT'S SIGNATURE
Other	CARDHOLDER'S SIGNATURE

1-12.2.11 Footer Information

- 1-12.2.11.1 A The format of the Footer Information block shall be as shown in figure 1-12.10.
- 1-12.2.11.2 A A receipt shall, if the transactions was not completed successfully, have a Footer Information block.

- 1-12.2.11.3 A A receipt shall, if a merchant as well as a cardholder receipt is printed, have a Footer Information block.

*****	FI1
INTERRUPTED - ERROR	FI2
*****	FI3
NO HOST RESPONSE RECVD.	FI4
ASW1 - ASW2: 1618	FI5
TVR:8008049040 TSI:3800	FI6
KEEP RECEIPT	FI7
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.10 - Footer Information Block

- 1-12.2.11.4 A A transaction that is not completed successfully shall have the lines FI1 - FI3. The content of line FI2 "Information footer text" shall be according to table 1-12.8 page 1-12-24. The information footer text shall be translated to the chosen language.

NOTE: The emphasizing of the text may be achieved in other ways, see section 1-12.2.2 page 1-12-7.

Table 1-12.8 - Termination cause and related Footer Text

Reason for termination	Information footer text
Transaction stopped/cancelled by cardholder or merchant	INTERRUPTED - CANCEL
Transaction declined by host, terminal or card.	DECLINED
Signature rejected by merchant.	SIGNATURE DECLINED
Failure of transaction/transmission	INTERRUPTED - ERROR

- 1-12.2.11.5 A If the merchant or the cardholder stops a transaction in progress before the cardholder has accepted the transaction by entering the PIN, the transaction shall be stopped/cancelled and the cardholder receipt shall indicate this.
- 1-12.2.11.6 A If the merchant or cardholder is able to stop a transaction in progress *after* the cardholder accepted the transaction by entering the PIN, the transaction shall be stopped/cancelled and the cardholder receipt shall indicate this.
- 1-12.2.11.7 B If a transaction is declined, either by the host as response to an online request or locally by the ICC or after local validation (e.g. Stop List check) then the cardholder receipt shall indicate this.
- 1-12.2.11.8 A If the signature was not accepted by the merchant, the cardholder receipt shall indicate that the signature was rejected.
- 1-12.2.11.9 A If a transactions fails, either due to communication errors on the host link, or due to technical problems internally in the terminal (e.g. communication between the ICC and the Card Reader), the receipt shall indicate this.

- 1-12.2.11.10 A If the terminal is an OTRS terminal, the evaluation of the transaction result shall be based on the ASW according to table 1-12.9.

Table 1-12.9 - Guideline for the Transaction Result

ASW1–ASW2 Range	Transaction Result
'0000' – '0000'	Approved
'0001' – '0FFF'	Failed
'1000' – '10FF'	Approved
'1100' – '11FF'	Failed
'1200' – '1274'	Declined
'1275' – '127F'	Stopped/Cancelled
'1280' – '15FF'	Declined
'1600' – '1702'	Failed
'1703' – '1703'	Stopped/Cancelled
'1704' – '1704'	Rejected Signature
'1705' – '1B85'	Failed
'1B86' – '1B86'	Stopped/Cancelled
'1B87' – '1BF1'	Failed
'1BF2' – '1BF2'	Stopped/Cancelled
'1BF3' – '1C4F'	Failed
'1C50' – '1CF2'	Stopped/Cancelled
'1CF3' – 'FFFF'	Failed

- 1-12.2.11.11 B A transaction that is not completed successfully shall have the line FI4. The content of the line shall be extended information on why the transaction was not completed successfully. Table 2-14.142 page 2-14-133, ASW1-ASW2 Converted to Message Codes, contains a list of possible texts. The line shall not disclose any information about suspected fraud etc.

NOTE: Information such as 'Suspected fraud', 'Card PIN blocked', 'Pick up card', 'Refer acquirer' alerting a possible fraudulent action is to be replaced with a neutral message such as 'Declined'.

- 1-12.2.11.12 A In an OTRS terminal, a transaction that is not completed successfully shall have the line FI5. The value printed shall be the first non-approved ASW returned from the PSAM.

- 1-12.2.11.13 A A receipt shall, for some regions, have a line FI6, "TVR/TSI". The line shall be printed, if it is a ICC transaction and the transaction is not completed successfully. The "TVR" shall have the header "TVR:" followed by the TVR in hexadecimal notation (10 digits). The "TSI" shall have a header of "TSI:" followed by the TSI in hexadecimal notation (4 digits). The TVR and TSI can, for an OTRS terminal be retrieved by issuing the *Get D/C properties* command with an identifier of '000B. See table 2-14.36. The call shall only be issued after the response to the *Complete* command has been received, and before the next command is initiated.

NOTE: There is no need for a delay after the *Complete* command if the transaction was failed or declined.

- 1-12.2.11.14 A A receipt shall for some regional versions have a line FI7, "Keep receipt". The text shall be printed in the chosen language.
- 1-12.2.11.15 A If the receipt is a part of a receipt pair, i.e. when a cardholder receipt as well as a merchant receipt is printed, then the receipt shall contain a "Recipient indicator" in line FI8. The content of the "Recipient indicator" shall be according to table 1-12.10. The text shall printed in the chosen language.

Table 1-12.10 - Recipient and related Indicator Text

Recipient	Recipient indicator
Cardholder	CARDHOLDER'S RECEIPT
Merchant	MERCHANT'S RECEIPT

1-12.2.12 Prepaid Card Information

- 1-12.2.12.1 A A receipt shall, if the transactions is a Prepaid MSC transaction contain a Prepaid Card Information block. The format of the Prepaid Card Information block shall be as shown in figure 1-12.11.
- 1-12.2.12.2 A A receipt shall, if it is a contactless transaction, and the card has an "Available Offline Spending Amount" (AOSA) contain a Prepaid Card Information block. The format of the Prepaid Card Information block shall be as shown in figure 1-12.11.

-----			PC1
			PC2
BALANCE	EUR	200,00	PC3
EXP. DATE		2012-04	PC4

Figure 1-12.11 - Prepaid Card Information Block

- 1-12.2.12.3 C A Prepaid Card receipt should, for formatting purposes, have lines PC1 and PC2.
- 1-12.2.12.4 A A Prepaid MSC receipt shall have the lines PC3 and PC4.
NOTE: This is the way to provide the cardholder with the balance information.
- 1-12.2.12.5 A Line PC3 shall hold the "Balance amount" information. It shall have a header text, a currency code and a balance. The header text shall be "BALANCE". The header text shall be translated to the chosen language. The currency code shall be the Alphabetic Currency Code of the merchant's local currency. The balance shall be the balance amount returned by the host. The balance shall be replaced by "blanks" if no amount information is returned from the host.
- 1-12.2.12.6 A Line PC4 shall hold the "Expiry Date" information. It shall have a header text and a expiry date. The header text shall be "EXP.DATE". The header text shall be printed in the chosen language. The expiry date shall be the expiry date returned by the host. The expiry date shall be replaced by "blanks" if no information is returned from the host.
NOTE: The "Expiry Date" is the expiry date of the balance on the card and not the expiry date of the physical card.

- 1-12.2.12.7 A A Prepaid ICC transaction here the card returns AOSA shall have the line PC3.
- 1-12.2.12.8 A Line PC3 shall hold the “available amount” information. It shall have a header text, a currency code and a spending amount. The header text shall be “BALANCE” or “AVAILABLE”. The header text shall be translated to the chosen language. The currency code shall be the Alphabetic Currency Code of the merchant's local currency. The balance shall be the balance amount returned by the card.

1-12.2.13 Receipt Footer

- 1-12.2.13.1 C A receipt may contain a Receipt Footer block. The receipt footer may contain information such as merchant logo, clerk identification, customer identification and specification of services. The structure of this block is outside the scope of this document.
- 1-12.2.13.2 C For receipts documenting the authorization of an amount that will cause a transaction at a later stage, the merchant's receipt should contain data elements in the receipt footer that makes it possible to identify the authorization.

NOTE: Car rental and hotels are examples of such transactions. They are, for OTRS terminals characterized as token based transactions.

1-12.2.14 Pre - receipt

Pre-receipts can be used for letting the cardholder make a number of decisions prior to generation of the actual receipt. Pre-receipts are used in DCC transactions to make the cardholder select the currency wanted. A pre-receipt can in a restaurant environment be used to have the cardholder specify the tips, even in non-DCC transactions.

- 1-12.2.14.1 C A pre-receipt for a non-DCC transaction shall contain;
- Merchant information
 - Header information
 - Amount information
- 1-12.2.14.2 A A pre-receipt shall, if it is generated before the Card scheme (PAN) is known, contain a Signature Informative block.
- 1-12.2.14.3 A A pre-receipt may require access to card information. A pre-receipt shall not cause the generation of a transaction.

1-12.3 DCC Receipt Layout

This section defines the layout of pre-receipts and receipts used at Dynamic Currency Conversion, DCC, transactions. A DCC transaction requires a pre-receipt as well as a receipt with special additional information. The requirements stated

in this section is an extension to requirements stated for non-DCC transactions in the previous part of this chapter.

1-12.3.1 Receipt Language

Receipts for DCC transactions will switch between the local language and English dependent on whether or not, the cardholder opts in for DCC.

- 1-12.3.1.1 A The terminal shall use English as the default language when generating Dynamic Currency Conversion, DCC, pre-receipts and receipts.
- 1-12.3.1.2 A The terminal shall *not* select a language based on the proposed DCC currency.
- 1-12.3.1.3 A Terminal shall, if the cardholder opts out of the DCC option, use the DCC receipt language rules for the remainder of the transaction.

NOTE: The fact that it has been detected that the card supports DCC may make it advantageous to the cardholder that English is used on the receipt.

1-12.3.2 Pre-receipt Structure

A generic example of a DCC pre-receipt is shown in figure 1-12.12 page 1-12-30. The pre-receipt shown contains all of the fields specific to a DCC-pre-receipt, but not all of the possible normal fields.

- 1-12.3.2.1 A A DCC pre-receipt shall have the following blocks.
- Merchant Information
 - Header Information
 - Amount Information
- The use of the different fields within a block is specified later in the sections.
- 1-12.3.2.2 C A DCC pre-receipt may have the following blocks.
- Receipt Header
 - Receipt Footer
- 1-12.3.2.3 A A DCC pre-receipt shall contain the same information in the Merchant Information block as a non-DCC receipt.
- 1-12.3.2.4 A A DCC pre-receipt shall not contain fields HI1 - HI2 of the information Header. A DCC pre-receipt shall contain lines HI3, HI4, HI5 and HI6. A DCC pre-receipt shall contain the lines HI7 - HI10 just as a non-DCC receipt.
- 1-12.3.2.5 A A DCC pre-receipt shall, after the Header Information block, contain a text (lines DC1 - DC3);
- 1-12.3.2.6 A The text shall for a Purchase, Authorization and capture transaction read;
- “You have the choice of paying your bill in either <local currency> or <cardholder's billing currency>”
- 1-12.3.2.7 A The text shall for a refund transaction read;

- "Use the same currency as in the original transaction"
- 1-12.3.2.8 A The <local currency> shall be the alphabetic currency code of the merchant's pricing currency and <cardholder's billing currency> shall be the alphabetic version of the currency code returned by the DCC application.
- 1-12.3.2.9 A A DCC pre-receipt shall contain two amount information blocks. The elements in the two blocks shall be the same. The first block shall state the amounts in the merchant's pricing currency (the local currency). The second block shall state the amounts in the cardholder's billing currency. The requirements for the generic Amount Information block shall apply.
- NOTE:** A DCC pre-receipt may include the fields for adding tips, lines AM11 - AM14 and thus at the same time being a tips pre-receipt.
- 1-12.3.2.10 C The lines DCC13 and DCC16 should be there for formatting purpose.
- 1-12.3.2.11 A There shall be the text "OR" between the two amount blocks, line DC15.
- 1-12.3.2.12 A There shall, after the second amount block, be a sentence on selection of currency, lines DC17 - D21, and a sentence on exchange rate, lines DC22 - DC25.
- 1-12.3.2.13 A The text on selection of currency shall for a cardholder's pre-receipt read;
- "Notify the staff of your choice of billing currency. The choice is final"
- 1-12.3.2.14 A The text on selection of currency shall for a merchant's re-fund pre-receipt read;
- "Notify the Cardholder of the amount and currency"
- 1-12.3.2.15 A The text on exchange rate shall read "The <rate type> exchange rate is based on <rate provider> rate, inclusive mark up <actual rate>". The <rate type> shall be according to table 1-12.11. The <rate provider> shall be the source of the exchange rate, i.e. "Reuters wholesale rate". The <actual rate> shall be the exchange rate provided from the <rate provider>.
- 1-12.3.2.16 B The printing of the exchange rate shall reflect, the precision of conversion rate from the service provider, limited to four digits after the decimal indicator ",,".

Table 1-12.11 - Transaction Type and Exchange Rate Type

Transaction Type, etc.	Related Exchange Rate Type
Authorization	REFERENCE
Other	GUARANTEED

NOTE: The selection between the two exchange rate types depends on whether or not the financial transaction is performed while the stated exchange rate is still valid.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
PRELIMINARY	HI4
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORISATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
YOU HAVE THE CHOICE OF	DC1
PAYING YOUR BILL IN	DC2
EITHER 'DKK' OR 'EUR'	DC3
	AM1
AMOUNT DKK 123456,78	AM2
SURCHARGE DKK 50,00	AM5
	AM8
TOTAL DKK 123506,78	AM9
	AM10

Figure 1-12.12 - Generic DCC Pre-receipt

EXTRA	DKK		AM11
		-----	AM12
TOTAL	DKK		AM13
		-----	AM14
			DC13
	OR		DC15
			DC16
AMOUNT	EUR	16552,94	AM2
SURCHARGE	EUR	6,70	AM5
		-----	AM8
TOTAL	EUR	16552,94	AM9
		-----	AM10
EXTRA	EUR		AM11
		-----	AM12
TOTAL	EUR		AM13
		-----	AM14
NOTIFY THE STAFF OF YOUR			DC17
CHOICE OF BILLING			DC18
CURRENCY.			DC19
THE CHOICE IS FINAL.			DC20
			DC21
THE GUARANTEED EXCHANGE			DC22
RATE IS BASED ON REUTERS			DC23
WHOLESALE RATE, INCLU-			DC24
SIVE MARK UP: 0,134078			DC25

Figure 1-12.12 - Generic DCC Pre-receipt (*concluded*)

1-12.3.3 Generic DCC Receipt Structure

An example of a DCC receipt is shown in figure 1-12.13 page 1-12-34 and figure 1-12.14 page 1-12-37. The receipt contains all of the fields specific to a DCC-receipt, but not all of the possible normal fields.

1-12.3.3.1 A A DCC receipt shall have the following blocks.

- Merchant Information
- Header Information
- Amount Information
- Transaction Information
- Signature Information
- Footer Information

The use of the different fields within a block is specified in the subsequent sections.

1-12.3.3.2 C A DCC receipt may have the following blocks.

- Receipt Header
- Receipt Footer

Merchant Information

1-12.3.3.3 A A DCC receipt shall contain the same information in the Merchant Information block as a non-DCC receipt.

Header Information

- 1-12.3.3.4 A A DCC receipt shall contain the same information in the Header Information block as a non-DCC receipt.
- The structure of the Amount Information block in a DCC receipt depend on whether the transaction is an authorization or financial transaction.

Amount Information, General

- 1-12.3.3.5 A A DCC receipt shall have up to two amount blocks. The first amount block, if present, shall be in the local currency. The second amount block shall be in the currency returned by the DCC application.

NOTE: The local currency is for DCC also known as the Merchant's Pricing currency. The currency returned by the DCC application is also known as Cardholder's Billing currency.

- 1-12.3.3.6 A For the first amount block, one of the following four, in requirement 1-12.3.3.7 to 1-12.3.3.10 mentioned, alternatives for indicating the amount(s) shall be used.
- 1-12.3.3.7 A If no surcharge is added, then only the line AMOUNT shall be printed.
- 1-12.3.3.8 C If surcharge is added, then the AMOUNT including surcharge may be printed, as the only value.
- 1-12.3.3.9 C If surcharge is added, then the AMOUNT including surcharge may be printed, as the only value. As a supplement a line with the text message 'INCLUDING SURCHARGE' may be added just below the amount value.
- 1-12.3.3.10 C If surcharge is added, then the AMOUNT (exclusive surcharge), the actual SURCHARGE and the TOTAL (in the local currency) may be printed on separate lines.
- 1-12.3.3.11 A For the first block, the amount shall include any services in the Merchants Pricing currency, that the cardholder has opted in for prior to the time of the transaction.
- 1-12.3.3.12 A For the second block, the SURCHARGE amount shall *not* be indicated in a separate line in the receipt. Only the amount, including any surcharge, shall be printed.
- 1-12.3.3.13 A For the second block, if the transaction is not a refund transaction, any EXTRA amount added by the cardholder, at the time of the transaction, shall be printed on the receipt in a separate line.
- NOTE:** After the exact amount in the Cardholders Billing currency has been presented to the cardholder, the cardholder may add an EXTRA amount.
- 1-12.3.3.14 A For the second block, if the transaction is a refund transaction and the receipt is to be handed over to the cardholder, only the total amount shall be printed.

NOTE: Even though the sub-amount shall not be printed on the receipt, these values may be entered by the

merchant or calculated automatically (Surcharge) based on the card data. The sub-amounts may e.g. be relevant for total reports or similar generated by the terminal

Amount Information, Authorization

- 1-12.3.3.15 A A DCC authorization receipt shall have up to two amount blocks. The content shall be according to table 1-12.12 page 1-12-33. The amount block(s) shall contain lines AM1, AM2 and AM14. The generic format of the amount information for an authorization receipt shall be as shown in figure 1-12.13 page 1-12-34 below.

Table 1-12.12 - Transaction Type and Amount Elements

Transaction Type	First amount block	Second amount block	Exchange rate
Authorization (merch. recpt)	Present	Present	Present
Authorization (cardh. recpt)	Absent	Present	Absent
Cancellation (auth)	Absent	Present	Absent

- 1-12.3.3.16 A The first amount block shall be in the local currency and the second amount block shall be in the currency returned by the DCC application.
- 1-12.3.3.17 A The exchange rate, lines DC21 - DC25 shall be a reference exchange rate. The information shall follow the same requirements as for a pre-receipt.

NOTE: Surcharge and corresponding total is not applicable in an Authorization.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT DKK 123456,78	AM2
-----	AM14
	DC13
OR	DC15
	DC16
AMOUNT EUR 16552,94	AM2
-----	AM14
	DC21
THE REFERENCE EXCHANGE	DC22
RATE IS BASED ON REUTERS	DC23
WHOLESALE RATE, INCLU-	DC24
SIVE MARK UP: 0,134078	DC25
	TR1
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
ACQUIRER NAME	TR7
I@1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
MERCHANT'S RECEIPT	FI8

Figure 1-12.13 - Generic DCC Authorization Receipt

Amount Information, Financial

The general definition of amount lines in the receipts may be found in figure 1-12.5 page 1-12-12.

The generic format, of the amount information in a DCC financial transaction, is shown in figure 1-12.14 page 1-12-37.

- 1-12.3.3.18 A The receipt for a DCC financial transaction receipt shall have two amount blocks.

- 1-12.3.3.19 A The first amount block shall be in the local currency, the Merchant's Pricing currency.
- 1-12.3.3.20 A The second amount block shall be in the currency returned by the DCC application, the Cardholder's Billing currency.
- 1-12.3.3.21 A The first amount block shall contain lines AM1, AM2 and AM14.
- 1-12.3.3.22 C The first amount block may contain lines AM4, AM5 and AM7, if VAT, surcharge or extra amount is relevant.
- 1-12.3.3.23 A If the first amount block contains either line AM5 or AM7 or both, the first block shall also contain total value in lines AM8 and AM9.
- Depending on the actual business environment, the cardholder may opt in for an extra amount (e.g. gratuity or a specific service fee) before the transaction total is added up and the currency conversion is computed.
- The cardholder may also add an extra amount (in the Cardholder's Billing currency) after currency conversion of the total amount is computed and presented to the cardholder.
- Addition of extra amounts may be possible in both situations. Surcharge and extra amounts may be contained in separate lines, AM5 and AM7, in both the first and the second amount block. The the amount values shall correspond, as defined in the following requirements.
- 1-12.3.3.24 A If line AM5 is contained in both the first and the second amount block, the amount values shall match according to the rules defined for currency conversion.
- 1-12.3.3.25 A If line AM7 is contained in both the first and the second amount block, the amount values shall match according to the rules defined for currency conversion.
- NOTE:** Only extra amounts added prior to the time of transaction may appear in line AM7 in both amount blocks.
- 1-12.3.3.26 A If an extra amount has been added in the Merchant's Pricing currency, but no extra amount has been added in the Cardholder's Billing currency, the extra amount shall appear on the receipts according to one of the following scenarios:
- The extra amount is part of the amount in line AM2 of both blocks.
 - The extra amount is specified in line AM7 of the first block, but is part of the amount in line AM2 of the second block.
 - The extra amount is specified in line AM7 of both blocks.
- 1-12.3.3.27 A If no extra amount has been added in the Merchant's Pricing currency, but an extra amount has been added in the Cardholder's Billing currency, the extra amount shall appear on the receipts according to the following scenario:
- The extra amount is not contained in the first block, but the extra amount is specified in line AM7 of the second block.
- 1-12.3.3.28 A If extra amounts has been added in both the Merchant's Pricing currency and the Cardholder's Billing currency, the extra amounts shall appear on the receipts according to both of the following requirements:

- The extra amount added in the Merchant's Pricing currency shall be part of the amount in line AM2 of both blocks.
- The extra amount added in the Cardholder's Billing currency shall not be contained in the first block, but the extra amount shall be specified in line AM7 of the second block.

NOTE: This imply that line AM7 will not appear in the first amount block, if extra amounts have been added both before and after currency conversion.

- 1-12.3.3.29 A The first amount block shall be followed by extended exchange rate information lines DC4 - DC9.
- 1-12.3.3.30 A The sentences on extended exchange rate information shall read "Exchange rate is based on <rate provider> wholesale rate at <yy-mm-dd>: Exchange rate <actual rate> Mark up on exchange rate <mark up on actual rate>". The <rate provider> shall be the source of the exchange rate, i.e. "Reuters wholesale rate". The <actual rate> shall be the exchange rate provided from the <rate provider>. The precision shall reflect the requirements in 1-12.3.2.16.
- 1-12.3.3.31 A The extended exchange rate shall be followed by the service provider information, lines DC10 - DC13. The service provider information shall read "This currency conversion service is provided by <conversion provider>". The <conversion provider> is defined in the regional requirements.
- 1-12.3.3.32 A The second amount block shall be prefixed by the text, line DC14, "Transaction currency".
- 1-12.3.3.33 A The second block shall contain all the relevant elements from a normal amount information block.

NOTE: There is no needs for lines AM9 - AM11 as this information could have been provided on the pre-receipt.

Transaction Information

- 1-12.3.3.34 A A DCC receipt shall contain the same information in part A of the Transaction Information block as a non-DCC receipt. See figure 1-12.6 page 1-12-14 for reference.
- 1-12.3.3.35 A A DCC receipt shall contain the same information in part B of the Transaction Information block as a non-DCC receipt. See figure 1-12.7 page 1-12-14 for reference

Signature Information

- 1-12.3.3.36 A A DCC authorization and purchase receipt shall contain a Signature Information block. The block shall be prefixed by the DCC acceptance statement. The statement shall read "I accept that <merchant> has offered me a choice of currencies for payment & this choice is final. I accept the conversion rate & final amount in <DCC currency>". The <merchant> shall be the same as stated in line MI1 or preprinted on the receipt. The <DCC currency> shall be the alphabetic version of the currency code returned by the DCC application.

- 1-12.3.3.37 A The Signature Information block shall contain the same information as a non-DCC signature transaction.

NOTE: A DCC receipt will not contain a Prepaid MSC Information block, as DCC is not applicable to prepaid cards.

Footer Information

- 1-12.3.3.38 A A DCC receipt shall contain the same information in the Footer Information block as a non-DCC receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT DKK 123456,78	AM2
SURCHARGE DKK 50,00	AM5
	AM8
TOTAL DKK 123506,78	AM9
	AM14
EXCHANGE RATE BASED ON	DC4
REUTERS WHOLESALE RATE	DC5
AT 2008-06-06:	DC6
EXCHANGE RATE: 0,123456	DC7
MARK UP ON	DC8
EXCHANGE RATE: 0,003704	DC9
THIS CURRENCY CONVERSION	DC10
SERVICE IS PROVIDED BY	DC11
TELLER A/S	DC12
	DC13
TRANSACTION CURRENCY	DC14
AMOUNT EUR 16552,94	AM2
SURCHARGE 6,70	AM5
EXTRA EUR 40,36	AM7
	AM8
TOTAL EUR 16600,00	AM9
	AM14
	TR1
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
ACQUIRER NAME	TR7

Figure 1-12.14 - Generic DCC Financial Receipt

I@1	ME.NO: 1234567890	TR8
I	ACCEPT THAT	DC26
	NETS - TESTSHOP	DC27
	HAS OFFERED ME A CHOICE	DC28
	OF CURRENCIES FOR	DC29
	PAYMENT & THIS CHOICE IS	DC30
	FINAL.	DC31
I	ACCEPT THE CONVERSION	DC32
	RATE & FINAL AMOUNT.	DC33
	IN 'EUR'	DC34
		SI25
	CARDHOLDER'S SIGNATURE:	SI26
		SI27
	SI28
ATC:	12345 AED: 061224	TR9
AID:	1234567890ABCDEF	TR10
PSAM:	1234567-1234567890	TR11
ARC:AB	STATUS:1234	TR12
AUT CODE:	1A2B3C	TR13
REF:123456	AUTHORIZED	TR14
	MERCHANT'S RECEIPT	FI8

Figure 1-12.14 - Generic DCC Financial Receipt
(concluded)

1-12.3.4 Compiled DCC Receipt Information

Figure 1-12.15 is a compiled list of all of the lines that may occur as DCC-related information in receipts and pre-receipts.

YOU HAVE THE CHOICE OF	DC1
PAYING YOUR BILL IN	DC2
EITHER 'DKK' OR 'EUR'	DC3
EXCHANGE RATE BASED ON	DC4
REUTERS WHOLESALE RATE	DC5
AT 2008-06-06:	DC6
EXCHANGE RATE: 0,123456	DC7
MARK UP ON	DC8
EXCHANGE RATE: 0,003704	DC9
THIS CURRENCY CONVERSION	DC10
SERVICE IS PROVIDED BY	DC11
TELLER A/S	DC12
	DC13
TRANSACTION CURRENCY	DC14
OR	DC15
	DC16
NOTIFY THE STAFF OF YOUR	DC17
CHOICE OF BILLING	DC18
CURRENCY.	DC19
THE CHOICE IS FINAL.	DC20
	DC21
THE GUARANTEED EXCHANGE	DC22
RATE IS BASED ON REUTERS	DC23
WHOLESALE RATE, INCLU-	DC24
SIVE MARK UP: 0,127160	DC25
I ACCEPT THAT	DC26
NETS - TESTSHOP	DC27
HAS OFFERED ME A CHOICE	DC28
OF CURRENCIES FOR	DC29
PAYMENT & THIS CHOICE IS	DC30
FINAL.	DC31
I ACCEPT THE CONVERSION	DC32
RATE & FINAL AMOUNT.	DC33
IN 'EUR'	DC34

Figure 1-12.15 - Compiled DCC Receipt Information

1-12.4 Examples of Receipts (Informative)

This section contains a series of examples of standard receipts. It has been included for information. For examples of receipts with regional texts, see the sections on regional requirements. Be aware that this is informative information only. The actual requirements are to be found in the preceding part of this section.

Table 1-12.13 - Examples of Receipts - Overview

Figure	Description
Receipt Type – Generic	
A	Purchase, full generic, all normal fields
B	Purchase, PIN, ICC, basic
C	Purchase, PIN, MSC, Copy, extended
D	Purchase, PIN, Fallback
E	Purchase, Signature, ICC, merchant
F	Purchase, Signature, ICC, cardholder
G	Refund, Cardholder's receipt
H	Cancellation of Purchase, PIN, ICC, cardholder
I	Original Authorization, Key Entered
J	Original Authorization, ICC, PIN, cardholder
K	Supplementary Authorization
L	Reversal of Authorization
M	Capture, No CVM, Signature, merchant
N	Capture, PIN, Signature, cardholder
O	Cash, ICC, Signature, merchant
P	Post registration, Purchase
Receipt – Unsuccessful	
Q	Failed transaction, error
R	Interrupted transaction, cancelled
S	Declined transaction, declined by host
T	Signature declined, declined by merchant
Prepaid MSC	
AA	Prepaid MSC, purchase w. cashback
AB	Prepaid MSC, load of card
AC	Prepaid MSC, balance only
AD	Prepaid MSC, offline purchase

Table 1-12.13 - Examples of Receipts - Overview
(concluded)

Figure	Description
	Pre–receipt and Receipt with Tips
BA	Pre–receipt, card known (2) or pre–receipt, card unknown, no surcharge (1)
BB	Pre–receipt, card unknown, surcharge possible (5)
BC	Receipt with on–display tips (3), PIN
BD	Receipt, adding tips after transaction (4), merchant
BE	Receipt, adding tips after transaction (4), cardholder
BF	Receipt, tips after transaction (4), final cardholder
BG	Receipt, after pre–receipt tips (2), cardholder
	DCC
CA	Pre–receipt, DCC, purchase
CB	Pre–receipt, DCC, authorization
CC	Pre–receipt, DCC, refund
CD	Pre–receipt, DCC, capture (finalize)
CE	Receipt, DCC, authorization, merchant
CF	Receipt, DCC, authorization, cardholder
CG	Receipt, DCC, Reversal of authorization, cardholder
CH	Receipt, DCC, capture (finalize), merchant
CI	Receipt, DCC, capture (finalize), cardholder
CJ	Receipt, DCC, purchase, PIN, merchant
CK	Receipt, DCC, purchase, PIN, cardholder

A cross reference between a subset of document types, terminal services, and recipients can be found in table 1-12.14.

Table 1-12.14 - Receipt Layouts

Type of document		Recipient	Terminal Services								
			Purchase	Original Auth.	Suppl. Auth.	Rever. Auth.	Finalize Payment	Refund	Cancellation	Cash	
Pre-receipt for TIPS decision		CH	BA				BA				
		ME									
Pre-receipt for TIPS decision (with surcharge rates)		CH	BB								
		ME									
Document for information only (Authorization)	PIN	CH		J		L					
		ME		(J)	(K)	(L)					
	Signature	CH		{ J }		(L)					
		ME		{(J)}	(K)	(L)					
Transaction Receipt	PIN	CH	B/C				N		H	{F}	
		ME	(B/C)				(N)		(H)	O	
	Signature	CH	F				N	G	H	{ F }	
		ME	E				M	{ B }	(H)	O	
	Tips and Signature	CH		BE			BF				
		ME		BD			(BF)				
	Tips	CH	BC/BG						{ H }		
		ME	(BC/BG)						{(H)}		
	Pre-receipt for DCC (and Tips) decision		CH	CA	CB			CD			CA
			ME						CC		
Document for information only (Authorization)	DCC and PIN	CH		CF		CG					
		ME		(CE)	(CE)	(CG)					
	DCC and Signature	CH		(CF)		(CG)					
		ME		(CE)	(CE)	(CG)					
Transaction Receipt	DCC and PIN	CH	CK				CI		{ CK }	{ CK }	
		ME	(CJ)				(CH)		{(CK)}	{ O }	
	DCC and Signature	CH	{ CK }				CI	{ CJ }	{ CK }	{ CK }	
		ME	{ CJ }				CH	{ (CK) }	{(CK)}	{ O }	

Table 1-12.14 - Receipt Layouts (*concluded*)

Type of document		Recipient	Terminal Function			
			Purchase (Contact)	Purchase (Contactless)	Load (Refund)	Balance (Original Auth.)
Prepaid MSC Transaction Receipt	No CVM Offline	CH	AD			
		ME				
	No CVM Online	CH	AA		AB	AC
		ME				
Legend:						
CH: Cardholder ME: Merchant						
Letters/Letter pairs (A – T and AA – AD, BA – BG and CA – CL) receipt references.						
White boxes: Mandatory receipts, reference formats described on the following pages.						
Letters/Letter pairs in (): Optional receipts.						
Letters/Letter pairs in {}: Closest reference receipt.						
Grey boxes: Receipts not applicable.						

1-12.4.1 A - Full Template

This is a full generic receipt template, holding all the lines defined for a generic receipt. Not all of these will appear at the same time. Some of the lines may hold multiple different messages. Only one of these is shown here. The receipts are included here as a reference source only.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI1
COPY	HI2
*****	HI3
PRELIMINARY	HI4
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORISATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM3
VAT INCL. EUR 12345,67	AM4
SURCHARGE EUR 2345,67	AM5
CASHBACK EUR 1000,00	AM6
EXTRA EUR 51,88	AM7
-----	AM8
TOTAL EUR 139200,00	AM9
-----	AM10
EXTRA EUR	AM11
-----	AM12
TOTAL EUR	AM13
-----	AM14
	AM15
PIN USED	TR1
MASTERCARD GOLD PSN:00	TR2
PAYM.CODE: 1234	TR3
DEBIT TRANSACTION	TR4
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
TELLER A/S	TR7
IB1 ME.NO: 1234567890	TR8

Figure 1-12.16 - Full Generic Receipt

	SI1
** VID EKSTRA **	SI2
KOM IHÅG NYT KVITTO	SI3
** WHEN TIPPING **	SI4
ASK FOR NEW RECEIPT	SI5
APPROVED FOR CREDITING	SI6
OF ACCOUNT	SI7
PRINTED DIGITS:	SI8
IDENTIFICATION:	SI9
(PASSPORT ETC:)	SI10
	SI11
.....	SI12
JURISDICTION OF ISSUE:	SI13
	SI14
**** PLEASE NOTICE ****	SI15
SURCHARGE WILL BE ADDED	SI16
IF PAYING BY CARD	SI17
AMERICAN EXPRESS: +4,56%	SI18
DINERS: +3,45%	SI19
JCB: +2,34%	SI20
MAESTRO: +1,23%	SI21
MASTERCARD: +2,34%	SI22
VISA: +2,34%	SI23
VISA ELECTRON: +2,34%	SI24
	SI25
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
*****	FI1
INTERRUPTED - ERROR	FI2
*****	FI3
NO HOST RESPONSE RECVD.	FI4
ASW1 - ASW2: 1618	FI5
TVR:8008049040 TSI:3800	FI6
KEEP RECEIPT	FI7
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.16 - Full Generic Receipt (*continued*)

-----			PC1
			PC2
BALANCE	EUR	200,00	PC3
EXP. DATE		2012-04	PC4
MAX DEPOSIT		150,00	CL1
AVAILABLE FUNDS		10,00	CL2
BALANCE BEFORE		40,00	CL3
CHARGE OF CARD		100,00	CL4
CARD BALANCE		123,00	CL5

Figure 1-12.16 - Full Generic Receipt (*concluded*)

1-12.4.2 B - Basic PIN Transaction, ICC.

A PIN purchase transaction, generating a minimal receipt, no extra features activated and formatting spaces removed.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
2008-04-23 13:04	HI10
PURCHASE EUR 123456,78	AM2
-----	AM14
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
IB1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.17 - Basic PIN Transaction Receipt, ICC

1-12.4.3 C - Extended PIN (Copy of Receipt) MSC

A (copy of a) receipt with a number of additional fields;

- VAT is to be printed on the receipt
- The transaction includes cashback
- There is a regional requirement for registration of PIN transaction.
- Payment code is used by the merchant.
- Account selection has been enabled/performed

ICC spec fields are not present, as this is a MSC transaction.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI1
COPY	HI2
*****	HI3
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 123456,78	AM2
VAT INCL. EUR 12345,67	AM4
CASHBACK EUR 1000,00	AM6
TOTAL EUR 139200,00	AM9
-----	AM14
PIN USED	TR1
MASTERCARD GOLD	TR2
PAYM. CODE: 1234	TR3
DEBIT TRANSACTION	TR4
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
TELLER A/S	TR7
DA1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.18 - Extended PIN Receipt, Copy of Original

1-12.4.4 D - PIN, ICC Fallback to MSC

A receipt with a fallback from ICC to MSC still using PIN as CVM. The deviations from an ICC receipt are;

- TR2, Card name from Host, and no PSN,
- Value in the TCC in line TR8,
- No ICC data, as magstripe was read, no TR9 and TR10.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 123456,78	AM2
VAT INCL. EUR 12345,67	AM4
CASHBACK EUR 1000,00	AM6
TOTAL EUR 124456,78	AM9
-----	AM14
PIN USED	TR1
MASTERCARD	TR2
PAYM. CODE: 1234	TR3
DEBIT TRANSACTION	TR4
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
EA1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.19 - Fallback Transaction Receipt, PIN

1-12.4.5 E - Signature, Merchant, VAT

A signature transaction will generally generate two receipts;

- The merchant's receipt, to be signed by the cardholder,
- The cardholder's initial receipt, handed over to the cardholder once the merchant's receipt has been signed.
- The receipt is shown with VAT printed

See receipts BD - BF for signature transactions where tips are added to the receipt after it has been signed.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 1234,56	AM2
-----	AM3
VAT INCL. EUR 12345,67	AM4
	AM15
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
I@1 ME.NO: 1234567890	TR8
	SI25
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
MERCHANT'S RECEIPT	FI8

Figure 1-12.20 - Signature Transaction, Merchant's Receipt

1-12.4.6 F - Signature, Cardholder, VAT

Cardholder's. Handed over to the cardholder after she/he has signed the merchant's receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 1234,56	AM2
-----	AM3
VAT INCL. EUR 12345,67	AM4
	AM15
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
I@1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.21 - Signature Transaction, Cardholder's Receipt

1-12.4.7 G - Refund

A refund transaction is always processed as a signature transaction. This receipt contains the optional "Approval message" in lines SI6 - SI7 and the "Clerk ID" in lines SI13 - SI15. Remark that the transaction is handled as a MSC transaction toward the host, even if an ICC is used.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI6
REFUND	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
REFUND EUR 123456,78	AM2
-----	AM14
MASTERCARD PSN:00	TR2
XXXX XXXX XXXX 1234	TR5
TERM: 1F2G3H4I-123456	TR6
I@1 ME.NO: 1234567890	TR8
APPROVED FOR CREDITING	SI6
OF ACCOUNT	SI7
	SI16
CLERK ID:	SI17
	SI15
MERCHANT'S SIGNATURE:	SI26
	SI27
.....	SI28
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.22 - Refund Transaction, Cardholder's Receipt

1-12.4.8 H - Cancellation

A cancellation receipt is always related to the immediately preceding transaction. It shall, aside from the 'Cancellation' label, be identical to the receipt from the cancelled transaction. Date, time and STAN shall be the same as in the cancelled transaction.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI1
CANCELLATION	HI4
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 123456,78	AM2
-----	AM14
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
IB1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.23 - Cancellation, Cardholder's Receipt

1-12.4.9 I - Original Authorization, Key Entered

An Original Authorization, generating a receipt is normally either a key entered transaction or a signature transaction. The one shown here is a Key entered transaction which can be used at the booking on a hotel. The card name is from the host response.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
MASTERCARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
TC1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.24 - Original Authorization, Key Entered, Merchant's Receipt

1-12.4.10 J - Original Authoriz, ICC, PIN, Cardholder

An Original authorization, may be based on a PIN transaction, as shown here. The card name is from the ICC data.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
IA1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.25 - Original Authorization, ICC and PIN, Cardholder's Receipt

1-12.4.11 K - Supplementary Authorization

A Supplementary Authorization, will be Key Entered, as the card is not present when the transaction is performed. The card data are retrieved from the token from the previous authorization. This may be the Original Authorization or a previous Supplementary Authorization. The TCC field TR8 reflects the conditions during the initial Original Authorization stored in the token. It does not reflect the way the Supplementary Authorization was made.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
IA1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.26 - Supplementary Authorization, Merchant's Receipt

1-12.4.12 L - Reversal of Authorization

The reversal of an Authorization does normally not involve the cardholder.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
REVERSAL (AUTH)	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
MASTERCARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
T@1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.27 - Reversal of Authorization

1-12.4.13 M - Capture, No CVM, Signature, Merchant

The receipt shall, if it is a Capture , always contain a signature field, as the Capture is performed without access to the card. The data necessary are retrieved from the token. ICC information will be retrieved, if the authorization was performed reading the chip. The TCC, line TR8, will reflect the conditions during the Original Authorization, in this case Key Entered information.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 16559,64	AM2
SURCHARGE EUR 40,36	AM5
-----	AM8
TOTAL EUR 16600,00	AM9
-----	AM14
	TR1
MASTERCARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
TC1 ME.NO: 1234567890	TR8
	SI25
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
MERCHANT'S RECEIPT	FI8

Figure 1-12.28 - Capture Receipt, Merchant.

1-12.4.14 N - Capture, PIN, Signature, Cardholder

The data necessary are retrieved from the token. ICC information will be retrieved, if the authorization was performed reading the chip. The TCC, line TR8, will reflect the conditions during the Original Authorization, in this case Chip and PIN.

The difference between the cardholder's and the merchant's receipt is that the Signature Information is removed.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	EUR	16559,64	AM2
EXTRA	EUR	40,36	AM5
		-----	AM8
TOTAL	EUR	16600,00	AM9
		-----	AM14
			TR1
MASTERCARD GOLD		PSN:00	TR2
XXXX XXXX XXXX XXX5 678			TR5
TERM: 1F2G3H4I-123456			TR6
IA1 ME.NO: 1234567890			TR8
ATC:12345 AED: 061224			TR9
AID: 1234567890ABCDEF			TR10
PSAM: 1234567-1234567890			TR11
ARC:AB STATUS:1234			TR12
AUT CODE: 1A2B3C			TR13
REF:123456 AUTHORIZED			TR14
CARDHOLDER'S RECEIPT			FI8

Figure 1-12.29 - Capture Receipt, Cardholder.

1-12.4.15 O - Cash, Signature

A receipt of this format shall be printed for PIN transactions as well. The actual number of fields to be filled in may depend on the card scheme and the acquirer requirements.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI6
CASH	HI7
*****	HI8
2008-04-23 13:04	HI10
CASH EUR 3000,00	AM2
-----	AM14
MASTERCARD GOLD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
D@1 ME.NO: 1234567890	TR8
	SI1
PRINTED DIGITS:	SI8
IDENTIFICATION:	SI9
(PASSPORT ETC:)	SI10
	SI11
.....	SI12
JURISDICTION OF ISSUE:	SI13
	SI14
.....	SI15
ID EXPIRY DATE:	SI16
	SI17
CLERK ID:	SI18
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.30 - Cash and Signature Transaction, Merchant's Receipt

1-12.4.16 P - Post Registration

The receipt of a post registration is a Key Entered No CVM transaction. It is based on Card information from a previous transaction. Neither the card nor the cardholder is present at the time of data entry.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 1234,56	AM2
-----	AM14
MASTERCARD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
TC1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.31 - Post Registration Receipt

1-12.4.17 Q - Failed Transaction

The format of a receipt is independent of the reason for the transaction being either declined or cancelled. The example displayed is based on an ICC transaction. Lines in the receipt, for which data are not available, are not printed.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	EUR	123456,78	AM2
VAT INCL.	EUR	12345,67	AM4
EXTRA	EUR	0,00	AM7
		-----	AM8
TOTAL	EUR	123456,78	AM9
		-----	AM14
VISA		PSN:00	TR2
XXXX XXXX XXXX 5678			TR5
TERM: 1F2G3H4I-123456			TR6
IA ME.NO: 1234567890			TR8
ATC:12345 AED: 061224			TR9
AID: 1234567890ABCDEF			TR10
PSAM: 1234567-1234567890			TR11
*****			FI1
INTERRUPTED - ERROR			FI2
*****			FI3
NO HOST RESPONSE RECVD.			FI4
ASW1 - ASW2: 1618			FI5

Figure 1-12.32 - Failed Transaction Receipt.

1-12.4.18 R - Interrupted Transaction

The format of a receipt is independent of the reason for the transaction being either declined or cancelled. The example displayed is based on an ICC transaction.

A large number of data are not available when a transaction is cancelled. Lines where data are not available are not printed.

This receipt contains the additional TVR and TSI information required in certain regions.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	EUR	123456,78	AM2
EXTRA	EUR	0,00	AM7
		-----	AM8
TOTAL	EUR	123456,78	AM9
		-----	AM14
TERM: 1F2G3H4I-			TR6
I ME.NO: 1234567890			TR8
*****			FI1
INTERRUPTED - CANCELLED			FI2
*****			FI3
			FI4
ASW1 - ASW2: 1275			FI5
TVR:8008049040 TSI:3800			FI6
KEEP RECEIPT			FI7
CARDHOLDER'S RECEIPT			FI8

Figure 1-12.33 - Interrupted Transaction Receipt.

1-12.4.19 S - Declined Transaction

The format of a receipt is independent of the reason for the transaction being either declined or cancelled. The example displayed is based on an MSC transaction. Lines where data are not available are blank. The blank lines may be omitted on the receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	IH9
2008-04-23 13:04	IH10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
VISA PSN:00	TR2
XXXX XXXX XXXX 5678	TR5
TERM: 1F2G3H4I-123456	TR6
DA1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1017	TR12
AUT CODE:	TR13
REF:	TR14
*****	FI1
DECLINED	FI2
*****	FI3
INCORRECT PIN	FI4
ASW1 - ASW2: 1221	FI5

Figure 1-12.34 - Declined Transaction Receipt

1-12.4.20 T - Signature Declined

A cardholder's final receipt. The signature has been declined by the merchant. Tips has been included in the amount, and the total is printed on the receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	IH9
2008-04-23 13:04	IH10
	AM1
PURCHASE EUR 1234,56	AM2
EXTRA EUR 65,44	AM7
-----	AM8
TOTAL EUR 1300,00	AM9
-----	AM14
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
I@1 ME.NO: 1234567890	TR8
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
*****	FI1
SIGNATURE DECLINED	FI2
*****	FI3
SIGNATURE DECLINED	FI4
ASW1 - ASW2: 1704	FI5
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.35 - Declined Signature Receipt.

1-12.4.21 AA - Prepaid MSC, Purch. with Cashback

This is a receipt for a transaction using a Prepaid MSC and returning balance information. Lines with ICC specific information are not present. It is a No CVM transaction.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	EUR	87,00	AM2
CASHBACK	EUR	13,00	AM6
		-----	AM8
TOTAL	EUR	100,00	AM9
		-----	AM14
NETS PREPAID CARD			TR2
XXXX XXXX XXXX XXX5 678			TR5
TERM: 1F2G3H4I-123456			TR6
DC1 ME.NO: 1234567890			TR8
PSAM: 1234567-1234567890			TR11
ARC: STATUS:1234			TR12
AUT CODE: 1A2B3C			TR13
REF:123456 AUTHORIZED			TR14
			PC1
			PC2
BALANCE	EUR	00,00	PC3
EXP.DATE		2012-04	PC4

Figure 1-12.36 - Prepaid MSC Purchase Receipt

1-12.4.22 AB - Prepaid MSC, Load

This is a receipt for a transaction loading a Prepaid MSC and returning balance information.

Empty lines in the Transaction Information block has been deleted from the receipt.

At the present, only empty Prepaid MSC can be loaded. It is a manual procedure to check the balance and ensure that the card is empty before loading the card.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
REFUND	EUR	200,00	AM2
		-----	AM14
NETS PREPAID CARD			TR2
XXXX XXXX XXXX XXX5 678			TR5
TERM: 1F2G3H4I-123456			TR6
DC5 ME.NO: 1234567890			TR8
PSAM: 1234567-1234567890			TR11
ARC: STATUS:1234			TR12
AUT CODE: 1A2B3C			TR13
REF:123456 AUTHORIZED			TR14
			PC1
			PC2
BALANCE	EUR	200,00	PC3
EXP.DATE		2012-04	PC4

Figure 1-12.37 - Prepaid MSC Load Receipt

1-12.4.23 AC - Prepaid MSC, Balance

The balance of a Prepaid MSC is obtained by performing an authorization of 0,00, and receiving the balance in the response. The amount 'authorized' shall not be displayed, as it is irrelevant to the cardholder.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR	AM2
-----	AM14
NETS PPREPAID CARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
DC1 ME.NO: 1234567890	TR7
PSAM: 1234567-1234567890	TR10
ARC: STATUS:1234	TR11
AUT CODE: 1A2B3C	TR12
REF:123456 AUTHORIZED	TR13
-----	PC1
	PC2
BALANCE EUR 183,15	PC3
EXP.DATE 2012-04	PC4

Figure 1-12.38 - Prepaid MSC, Balance.

1-12.4.24 AD - Prepaid MSC, Offline Purch. with Cashback

This is a receipt for an offline transaction using a Prepaid MSC. The balance information is not returned and shall be displayed as blanks, as no Host connection is obtained. Outstanding Host information is to be replaced with blanks and empty lines may be omitted.

The card name will be a generic name returned by the PSAM, based on it's internal scheme information.

The card should always be retained by the merchant at an offline purchase, giving any remaining funds to the cardholder as cashback.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	EUR	67,00	AM2
CASHBACK	EUR	33,00	AM6
		-----	AM8
TOTAL	EUR	100,00	AM9
		-----	AM14
<PREPAID CARD>			TR2
XXXX XXXX XXXX XXX5 678			TR5
TERM: 1F2G3H4I-123456			TR6
DC5 ME.NO: 1234567890			TR8
PSAM: 1234567-1234567890			TR11
ARC: STATUS:			TR12
REF: AUTHORIZED			TR14
			PC1
			PC2
BALANCE	EUR		PC3
EXP.DATE			PC4

Figure 1-12.39 - Prepaid MSC Offline Purchase Receipt

1-12.4.25 BA - Pre-receipt, no Surch./Surch. and Card known

A pre-receipt may be generated, based on a standard receipt. This is the version where the card is known in advance. This makes it possible to include surcharges on the pre-receipt.

The pre-receipt, with line AM4 omitted, or the value of 0,00 may be used when there are no surcharges, independent of whether or not the card is known in advance.

This pre-receipt makes it possible to record information about gratuity/extra before the actual transaction is performed.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
*****			HI3
PRELIMINARY			HI4
THIS IS NOT A RECEIPT			HI5
*****			HI6
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	EUR	1234,56	AM2
VAT INCL.	EUR	123,45	AM4
SURCHARGE	EUR	23,45	AM5
		-----	AM8
TOTAL	EUR	1381,46	AM9
		-----	AM10
EXTRA	EUR		AM11
		-----	AM12
TOTAL	EUR		AM13
		-----	AM14

Figure 1-12.40 - Plain Pre-receipt with Surcharge

1-12.4.26 BB - Pre-receipt, Card unknown, Surch.

A pre-receipt may be generated, based on a standard no CVM receipt. This is the version where the card is not known in advance, and it is not possible to specify surcharges in advance.

This pre-receipt makes it possible to record information about gratuity/extra before the transaction is performed.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
PRELIMINARY	HI4
THIS IS NOT A RECEIPT	HI5
*****	HI6
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
	AM8
EXTRA EUR	AM11
	AM12
TOTAL EUR	AM13
	AM14
**** PLEASE NOTICE ****	SI15
SURCHARGE WILL BE ADDED	SI16
IF PAYING BY CARD	SI17
AMERICAN EXPRESS: +4,56%	SI18
DINERS: +3,45%	SI19
JCB: +2,34%	SI20
MAESTRO: +1,23%	SI21
MASTERCARD: +2,34%	SI22
VISA: +2,34%	SI23
VISA ELECTRON: +2,34%	SI24
	SI25

Figure 1-12.41 - Plain Pre-receipt prior to Surcharge

1-12.4.27 BC - Receipt after On-display Tips, PIN

A receipt with an additional field;

- The transaction includes extra/gratuuity, pre-registered on the receipt.

ICC specif fields are not present, as this is a MSC transaction.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
2008-04-23	13:04		HI10
			AM1
PURCHASE	EUR	123456,78	AM2
EXTRA	EUR	6543,22	AM7
TOTAL	EUR	130000,00	AM8
		-----	AM14
MASTERCARD GOLD			TR2
XXXX XXXX XXXX XXX5 678			TR5
TERM: 1F2G3H4I-123456			TR6
DA1 ME.NO: 1234567890			TR8
PSAM: 1234567-1234567890			TR11
ARC:AB	STATUS:1234		TR12
AUT CODE: 1A2B3C			TR13
REF:123456	AUTHORIZED		TR14

Figure 1-12.42 - PIN and On-display Tips, Cardholder's Receipt

1-12.4.28 BD - Receipt, Tips after Trans, Merchant

A signature transaction with late tips may generate up to three receipts;

- The merchant's receipt, to be signed by the cardholder,
- The cardholder's initial receipt, handed over to the cardholder once the merchant's receipt has been signed.
- The, optional, final cardholder's receipt including tips.

Remark that the two initial receipts are based on an authorization. The example below has the doubled "Tips Informative message", SI 2 - 3 and SI 4 - 5.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23	13:04
	HI10
	AM1
PURCHASE EUR 1234,56	AM2
EXTRA EUR	AM11

	AM12
TOTAL EUR	AM13

	AM14
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
I@1 ME.NO: 1234567890	TR8
	SI1
** VID EKSTRA **	SI2
KOM IHÅG NYT KVITTO	SI3
** WHEN TIPPING **	SI4
ASK FOR NEW RECEIPT	SI5
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
MERCHANT'S RECEIPT	FI8

Figure 1-12.43 - Signature Transaction with Tips, Merchant's Receipt

1-12.4.29 BE - Receipt, Tips after Trans, Cardholder's

cardholder's initial receipt. Handed over to the cardholder after he has signed the merchant's receipt.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
PURCHASE	EUR	1234,56	AM2
EXTRA	EUR		AM11
		-----	AM12
TOTAL	EUR		AM13
		-----	AM14
MASTERCARD GOLD	PSN:00		TR2
XXXX XXXX XXXX XXX5	678		TR5
TERM:	1F2G3H4I-123456		TR6
I@1	ME.NO: 1234567890		TR8
ATC:12345	AED: 061224		TR9
AID:	1234567890ABCDEF		TR10
PSAM:	1234567-1234567890		TR11
ARC:AB	STATUS:1234		TR12
AUT CODE:	1A2B3C		TR13
REF:123456	AUTHORIZED		TR14
CARDHOLDER'S RECEIPT			FI8

Figure 1-12.44 - Signature Transaction, Cardholder's Receipt, before Tips

1-12.4.30 BF - Receipt, Tips after Trans, Cardholder's, Final

Cardholder's final receipt. Tips has been included in the amount, and the total is printed on the receipt.

NETS - TESTSHOP	MI1		
Lautrupbjerg 10	MI2		
2750 Ballerup	MI3		
Phone: (+45) 44 68 44 68	MI4		
Bus.Reg.No: 1234567890	MI5		
	HI9		
2008-04-23	13:04	HI10	
		AM1	
PURCHASE	EUR	1234,56	AM2
EXTRA	EUR	65,44	AM7
		-----	AM8
TOTAL	EUR	1300,00	AM9
		-----	AM14
MASTERCARD GOLD	PSN:00	TR2	
XXXX XXXX XXXX XXX5 678		TR5	
TERM: 1F2G3H4I-123456		TR6	
I@1 ME.NO: 1234567890		TR8	
ATC:12345 AED: 061224		TR9	
AID: 1234567890ABCDEF		TR10	
PSAM: 1234567-1234567890		TR11	
ARC:AB STATUS:1234		TR12	
AUT CODE: 1A2B3C		TR13	
REF:123456 AUTHORIZED		TR14	
CARDHOLDER'S RECEIPT		FI8	

Figure 1-12.45 - Signature Transaction, Cardholder's Receipt - Final.

1-12.4.31 BG - Receipt after Pre-rec. Tips, Sign, Merchant.

This is the receipt generated, when tips has been added using a pre-receipt.

- The transaction includes extra/gratuity, pre-registered on the receipt.
- There is no prompt for requesting a final receipt, SI1 - SI5 as no information is added after this receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
2008-04-23 13:04	HI10
	AM1
PURCHASE EUR 123456,78	AM2
EXTRA EUR 6543,22	AM7
TOTAL EUR 130000,00	AM8
-----	AM14
MASTERCARD GOLD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
D@1 ME.NO: 1234567890	TR8
CARDHOLDER'S SIGNATURE:	SI26
	SI27
.....	SI28
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.46 - Receipt after Pre-receipt, Signature, Merchant's Receipt

1-12.4.32 CA - Pre-receipt, DCC Purchase

A pre-receipt may be generated, based on a standard receipt. This is the version for DCC at purchase.

A pre-receipt, with lines AM4 and AM7 omitted, or the value of 0,00 may be used when there are no surcharges.

The lines AM10 through AM13 may be omitted if tips is not to be added.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
*****			HI3
PRELIMINARY			HI4
THIS IS NOT A RECEIPT			HI5
*****			HI6
			HI9
2008-04-23		13:04	HI10
YOU HAVE THE CHOICE OF			DC1
PAYING YOUR BILL IN			DC2
EITHER 'DKK' OR 'EUR'			DC3
			AM1
AMOUNT DKK 123456,78			AM2
SURCHARGE DKK 50,00			AM5
		-----	AM8
TOTAL DKK 123506,78			AM9
		-----	AM10
EXTRA DKK			AM11
		-----	AM12
TOTAL DKK			AM13
		-----	AM14
			DC13
		OR	DC15
			DC16
AMOUNT EUR 16552,94			AM2
SURCHARGE EUR 6,70			AM5
		-----	AM8
TOTAL EUR 16559,64			AM9
		-----	AM10
EXTRA EUR			AM11
		-----	AM12
TOTAL EUR			AM13
		-----	AM14

Figure 1-12.47 - DCC Pre-receipt Purchase with Tips

NOTIFY THE STAFF OF YOUR	DC17
CHOICE OF BILLING	DC18
CURRENCY.	DC19
THE CHOICE IS FINAL.	DC20
	DC21
THE GUARANTEED EXCHANGE	DC22
RATE IS BASED ON REUTERS	DC23
WHOLESALE RATE, INCLU-	DC24
SIVE MARK UP: 0,134078	DC25

Figure 1-12.47 - DCC Pre-receipt Purchase with Tips
(concluded)

1-12.4.33 CB - Pre-receipt, DCC Authorization

A pre-receipt may be generated, based on a standard receipt. This is the version for DCC. Remark that the exchange rate, DCC22 , shall be 'REFERENCE' as the actual exchange rate is the rate at the time of the capture.

Surcharges and gratuity/tips are not applicable to an authorization.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
PRELIMINARY	HI4
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
YOU HAVE THE CHOICE OF	DC1
PAYING YOUR BILL IN	DC2
EITHER 'DKK' OR 'EUR'	DC3
	AM1
AMOUNT DKK 123456,78	AM2
-----	AM14
	DC13
OR	DC15
	DC16
AMOUNT EUR 16552,94	AM2
-----	AM14
NOTIFY THE STAFF OF YOUR	DC17
CHOICE OF BILLING	DC18
CURRENCY.	DC19
THE CHOICE IS FINAL.	DC20
	DC21
THE REFERENCE EXCHANGE	DC22
RATE IS BASED ON REUTERS	DC23
WHOLESALE RATE, INCLU-	DC24
SIVE MARK UP: 0,134078	DC25

Figure 1-12.48 - Generic DCC Pre-receipt, Authorization

1-12.4.34 CC - Pre-receipt, DCC Refund

A pre-receipt may be generated, based on a standard receipt. This is the version for DCC.

Surcharges and gratuity/tips are not applicable to a refund transaction. Remark that the selection request, DC1 - DC2 and the notification information, lines DC17 - DC21 differs from the one used for Purchase and Authorization.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
PRELIMINARY	HI4
THIS IS NOT A RECEIPT	HI5
*****	HI6
REFUND	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
USE SAME CURRENCY AS IN	DC1
THE ORIGINAL TRANSACTION	DC2
	AM1
AMOUNT DKK 123456,78	AM2
-----	AM14
	DC13
OR	DC15
	DC16
AMOUNT EUR 16552,94	AM2
-----	AM14
NOTIFY THE CARDHOLDER OF	DC17
THE AMOUNT AND CURRENCY	DC18
	DC21
THE GUARANTEED EXCHANGE	DC22
RATE IS BASED ON REUTERS	DC23
WHOLESALE RATE, INCLU-	DC24
SIVE MARK UP: 0,134078	DC25

Figure 1-12.49 - DCC Pre-receipt, Refund

1-12.4.35 CD - Pre-receipt, DCC Capture

This pre-receipt does not contain the possibility of selecting currency, as this selection process was performed during the previous authorization. The currency to use, shall be the currency selected in the authorization.

The language of the receipt shall be English if the terminal does not support the preferred language of the card, as it is an DCC pre-receipt. The format of the pre-receipt is identical to normal non-DCC pre-receipts.

This pre-receipt makes it possible to record information about gratuity/extra before the actual transaction is performed.

PBS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
*****			HI3
PRELIMINARY			HI4
THIS IS NOT A RECEIPT			HI5
*****			HI6
			HI9
2008-04-23		13:04	H10
			AM1
AMOUNT	EUR	1234,56	AM2
SURCHARGE	EUR	23,45	AM5
		-----	AM8
TOTAL	EUR	1381,46	AM9
		-----	AM10
EXTRA	EUR		AM11
		-----	AM12
TOTAL	EUR		AM13
		-----	AM14

Figure 1-12.50 - DCC Pre-receipt Capture

1-12.4.36 CE - DCC, Authorization, Merchant

A DCC Authorization receipt for the merchant will show the amount in the merchant's pricing currency as well as in the cardholder's billing currency. This format is applicable to Original/Extended Authorizations as well as additional Authorizations. An additional Authorization will normally be performed without the card being present, i.e. as a key entered transaction.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT DKK 123456,78	AM2
-----	AM14
	DC13
OR	DC15
	DC16
AMOUNT EUR 16552,94	AM2
-----	AM14
	DC21
THE REFERENCE EXCHANGE	DC22
RATE IS BASED ON REUTERS	DC23
WHOLESALE RATE, INCLU-	DC24
SIVE MARK UP: 0,134078	DC25
	TR1
MASTERCARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
T@1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.51 - DCC Authorization Receipt, Merchant

1-12.4.37 CF - DCC, Authorization, Cardholder

A DCC Authorization receipt for the cardholder will only show the amount in the cardholder's billing currency, as the reservation on the cardholder's account is performed directly in the cardholder's billing currency. This format is applicable to Original/Extended Authorization as well as to additional Authorization. An additional Authorization will normally be performed without the card being present, i.e. as a key entered transaction.

The format of the receipt is identical to the format of a non-DCC receipt, except that the default language of the receipt will be English and that the currency always will be the cardholder's billing currency.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
AUTHORIZATION ONLY	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
MASTERCARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
TC1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.52 - DCC, Authorization, Key Entered, Merchant's

1-12.4.38 CG - DCC, Reversal of Authorization

The reversal of an Authorization does not normally involve the cardholder. It will always be a key entered transaction.

The format of the receipt is identical to the format of a non-DCC receipt, except that the language of the receipt will be the preferred language of the card or English and that the currency always will be the cardholder's billing currency, as the reservation was made in this currency.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
*****	HI3
THIS IS NOT A RECEIPT	HI5
*****	HI6
REVERSAL (AUTH)	HI7
*****	HI8
	HI9
2008-04-23 13:04	HI10
	AM1
AMOUNT EUR 123456,78	AM2
-----	AM14
MASTERCARD	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
T@1 ME.NO: 1234567890	TR8
PSAM: 1234567-1234567890	TR11
ARC: STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14

Figure 1-12.53 - DCC, Reversal of Authorization

1-12.4.39 CH - DCC, Capture, Merchant

A DCC receipt for the merchant will show the amount in the merchant's pricing currency as well as in the cardholder's billing currency. This general format is applicable to a plain purchase as well as to the capture of a token transaction. The current receipt is a capture receipt. For a capture, the header on line AM2 shall read "AMOUNT" instead of "PURCHASE".

The receipt shall, if it is a Capture, always contain a signature field, as the Capture is performed without access to the card. The data necessary are retrieved from the token. ICC information will be retrieved, if the authorization was performed reading the chip. The TCC, line TR8, will reflect the conditions during the Original Authorization.

Remark that the surcharge is not present in the second amount block, and that the extra is present only in the second block.

It is not possible to add gratuity/tips on a DCC receipt. If this was not added during the authorization, then it must be added using an intermediate pre-receipt as specified in section 1-12.4.35.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	DKK	123456,78	AM2
SURCHARGE	DKK	50,00	AM5
		-----	AM8
TOTAL	DKK	123506,78	AM9
		-----	AM14
EXCHANGE RATE BASED ON			DC4
REUTERS WHOLESALE RATE			DC5
AT 2008-06-06:			DC6
EXCHANGE RATE:		0,123456	DC7
MARK UP ON			DC8
EXCHANGE RATE:		0,003704	DC9
THIS CURRENCY CONVERSION			DC10
SERVICE IS PROVIDED BY			DC11
TELLER A/S			DC12
			DC13
TRANSACTION CURRENCY			DC14
AMOUNT	EUR	16559,64	AM2
EXTRA	EUR	40,36	AM7

Figure 1-12.54 - DCC Capture Receipt, Merchant

	-----	AM8
TOTAL	EUR 16600,00	AM9
	-----	AM14
		TR1
MASTERCARD GOLD	PSN:00	TR2
XXXX XXXX XXXX XXX5	678	TR5
TERM:	1F2G3H4I-123456	TR6
IA1 ME.NO:	1234567890	TR8
I ACCEPT THAT		DC26
NETS - TESTSHOP		DC27
HAS OFFERED ME A CHOICE		DC28
OF CURRENCIES FOR		DC29
PAYMENT & THIS CHOICE IS		DC30
FINAL.		DC31
I ACCEPT THE CONVERSION		DC32
RATE & FINAL AMOUNT.		DC33
IN 'EUR'		DC34
		SI25
CARDHOLDER'S SIGNATURE:		SI26
		SI27
.....		SI28
ATC:12345	AED: 061224	TR9
AID:	1234567890ABCDEF	TR10
PSAM:	1234567-1234567890	TR11
ARC:AB	STATUS:1234	TR12
AUT CODE:	1A2B3C	TR13
REF:123456	AUTHORIZED	TR14
MERCHANT'S RECEIPT		FI8

Figure 1-12.54 - DCC capture receipt, merchant
(concluded)

1-12.4.40 CI - DCC, Capture, Cardholder

A DCC receipt for the cardholder will show the amount in the merchant's pricing currency as well as in the cardholder's billing currency. This general format is applicable to a plain purchase as well as to the capture of token transaction. For a purchase, the header on line AM2 shall read "PURCHASE" instead.

The difference between the cardholder's and the merchant's receipt is the Signature Information block for the merchant.

NETS - TESTSHOP			MI1
Lautrupbjerg 10			MI2
2750 Ballerup			MI3
Phone: (+45) 44 68 44 68			MI4
Bus.Reg.No: 1234567890			MI5
			HI9
2008-04-23		13:04	HI10
			AM1
AMOUNT	DKK	123456,78	AM2
SURCHARGE	DKK	50,00	AM5
		-----	AM8
TOTAL	DKK	123506,78	AM9
		-----	AM14
EXCHANGE RATE BASED ON			DC4
REUTERS WHOLESALE RATE			DC5
AT 2008-06-06:			DC6
EXCHANGE RATE:		0,123456	DC7
MARK UP ON			DC8
EXCHANGE RATE:		0,003704	DC9
THIS CURRENCY CONVERSION			DC10
SERVICE IS PROVIDED BY			DC11
TELLER A/S			DC12
			DC13
TRANSACTION CURRENCY			DC14
AMOUNT	EUR	16559,64	AM2
EXTRA	EUR	40,36	AM5
		-----	AM8
TOTAL	EUR	16600,00	AM9
		-----	AM14
			TR1
MASTERCARD GOLD	PSN:00		TR2
XXXX XXXX XXXX XXX5 678			TR5
TERM:		1F2G3H4I-123456	TR6
IA1	ME.NO:	1234567890	TR8
I ACCEPT THAT			DC26

Figure 1-12.55 - DCC capture receipt, cardholder

NETS - TESTSHOP	DC27
HAS OFFERED ME A CHOICE	DC28
OF CURRENCIES FOR	DC29
PAYMENT & THIS CHOICE IS	DC30
FINAL.	DC31
I ACCEPT THE CONVERSION	DC32
RATE & FINAL AMOUNT.	DC33
IN 'EUR'	DC34
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.55 - DCC capture receipt, cardholder
(concluded)

1-12.4.41 CJ - DCC, Refund, Cardholder

A DCC receipt for the merchant will show the amount in the merchant's pricing currency as well as in the cardholder's billing currency. This general format is applicable to a plain purchase as well as to the capture of a token transaction. The current receipt is a purchase receipt. For a capture, the header on line AM2 shall read "AMOUNT" instead.

It is not possible to add gratuity/tips on a final DCC receipt. This is to be added either on the pre-receipt used to select currency, or on an extra pre-receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
REFUND DKK 123456,78	AM2
-----	AM14
EXCHANGE RATE BASED ON	DC4
REUTERS WHOLESALE RATE	DC5
AT 2008-06-06:	DC6
EXCHANGE RATE: 0,123456	DC7
MARK UP ON	DC8
EXCHANGE RATE: 0,003704	DC9
THIS CURRENCY CONVERSION	DC10
SERVICE IS PROVIDED BY	DC11
TELLER A/S	DC12
	DC13
TRANSACTION CURRENCY	DC14
REFUND EUR 16559,64	AM2
-----	AM8
TOTAL EUR 16599,64	AM9
-----	AM14
	TR1
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
I@5 ME.NO: 1234567890	TR8
	SI25
MERCHANTS'S SIGNATURE:	SI26
	SI27
.....	SI28

Figure 1-12.56 - DCC refund receipt, cardholder

ATC:12345	AED: 061224	TR9
AID:	1234567890ABCDEF	TR10
PSAM:	1234567-1234567890	TR11
ARC:AB	STATUS:1234	TR12
AUT CODE:	1A2B3C	TR13
REF:123456	AUTHORIZED	TR14
CARDHOLDER'S RECEIPT		FI8

Figure 1-12.56 - DCC refund receipt, cardholder
(concluded)

1-12.4.42 CK - DCC, Purchase, Merchant

A DCC receipt for the merchant will show the amount in the merchant's pricing currency as well as in the cardholder's billing currency. This general format is applicable to a plain purchase as well as to the capture of a token transaction. The current receipt is a purchase receipt. For a capture, the header on line AM2 shall read "AMOUNT" instead.

It is not possible to add gratuity/tips on a final DCC receipt. This is to be added either on the pre-receipt used to select currency, or on an extra pre-receipt.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE DKK 123456,78	AM2
SURCHARGE DKK 50,00	AM5
-----	AM8
TOTAL DKK 123506,78	AM9
-----	AM14
EXCHANGE RATE BASED ON	DC4
REUTERS WHOLESALE RATE	DC5
AT 2008-06-06:	DC6
EXCHANGE RATE: 0,123456	DC7
MARK UP ON	DC8
EXCHANGE RATE: 0,003704	DC9
THIS CURRENCY CONVERSION	DC10
SERVICE IS PROVIDED BY	DC11
TELLER A/S	DC12
	DC13
TRANSACTION CURRENCY	DC14
PURCHASE EUR 16559,64	AM2
-----	AM8
TOTAL EUR 16599,64	AM9
-----	AM14
	TR1
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
IA1 ME.NO: 1234567890	TR8
I ACCEPT THAT	DC26

Figure 1-12.57 - DCC purchase receipt, merchant's

NETS - TESTSHOP	DC27
HAS OFFERED ME A CHOICE	DC28
OF CURRENCIES FOR	DC29
PAYMENT & THIS CHOICE IS	DC30
FINAL.	DC31
I ACCEPT THE CONVERSION	DC32
RATE & FINAL AMOUNT.	DC33
IN 'EUR'	DC34
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
MERCHANT'S RECEIPT	FI8

Figure 1-12.57 - DCC purchase receipt, merchant's
(concluded)

1-12.4.43 CM - DCC, Purchase, Cardholder

A DCC receipt for the cardholder will show the amount in the merchant's pricing currency as well as in the cardholder's billing currency. This general format is applicable to a plain purchase as well as to the capture of token transaction. For a capture, the header on line AM2 shall read "AMOUNT".

There is no difference between the cardholder's and the merchant's receipt. There shall be no signature block, if it is a PIN transaction.

NETS - TESTSHOP	MI1
Lautrupbjerg 10	MI2
2750 Ballerup	MI3
Phone: (+45) 44 68 44 68	MI4
Bus.Reg.No: 1234567890	MI5
	HI9
2008-04-23 13:04	HI10
	AM1
PURCHASE DKK 123456,78	AM2
SURCHARGE DKK 50,00	AM5
	AM8
TOTAL DKK 123506,78	AM9
	AM14
EXCHANGE RATE BASED ON	DC4
REUTERS WHOLESALE RATE	DC5
AT 2008-06-06:	DC6
EXCHANGE RATE: 0,123456	DC7
MARK UP ON	DC8
EXCHANGE RATE: 0,003704	DC9
THIS CURRENCY CONVERSION	DC10
SERVICE IS PROVIDED BY	DC11
TELLER A/S	DC12
	DC13
TRANSACTION CURRENCY	DC14
PURCHASE EUR 16552,94	AM2
	AM8
TOTAL EUR 16600,00	AM9
	AM14
	TR1
MASTERCARD GOLD PSN:00	TR2
XXXX XXXX XXXX XXX5 678	TR5
TERM: 1F2G3H4I-123456	TR6
IA1 ME.NO: 1234567890	TR8
I ACCEPT THAT	DC26

Figure 1-12.58 - DCC purchase receipt, cardholder

NETS - TESTSHOP	DC27
HAS OFFERED ME A CHOICE	DC28
OF CURRENCIES FOR	DC29
PAYMENT & THIS CHOICE IS	DC30
FINAL.	DC31
I ACCEPT THE CONVERSION	DC32
RATE & FINAL AMOUNT.	DC33
IN 'EUR'	DC34
ATC:12345 AED: 061224	TR9
AID: 1234567890ABCDEF	TR10
PSAM: 1234567-1234567890	TR11
ARC:AB STATUS:1234	TR12
AUT CODE: 1A2B3C	TR13
REF:123456 AUTHORIZED	TR14
CARDHOLDER'S RECEIPT	FI8

Figure 1-12.58 - DCC purchase receipt, cardholder
(concluded)

1-12.4.44 English Receipt Texts

Table 1-15.5 page 1-15-13 defines the English reference texts that shall be used when printing receipts. A table with the corresponding national texts are found in section 1-15.

The content of the table is as follows;

- The first column refers to the line numbers displayed in the generic receipt format, like 'IH5'. The number may be followed by a letter if multiple texts are possible. If the same element is used in multiple lines, then both entries will be shown, separated by a '/'.
• The second column holds the logical name of the element. The name is only mentioned first time, if multiple entries exists for a receipt line. An example of this are the lines 'AM2a' and 'AM2b'.
• The third column holds the English (reference) text.
• The fourth column holds the text in the regional language. The column may hold the entry <blank> if the element is not used in the specific language.
• The text specified in column three and four may span two or more lines. New line is indicated by a '\n' in the text.

Table 1-12.15 - Messages for printing (reference)

Receipt Line	Element	English	National
'MI4'	Phone	Phone:	
'MI5'	Business Reg. number	Bus.Reg.No:	
'HI2'	Copy indicator	Copy	
'HI4a'	Prelim/post indicator	Preliminary	
'HI4b'	Prelim/post indicator	Post registration	
'HI4c'	Cancellation indicator	Cancellation	
'IH5'	Non-financial indicator	This is not a receipt	
'HI7a'	Transaction indicator	Authorization only	
'HI7b'		Refund	
'HI7c'		Reversal (auth)	
'HI7d'		Cancellation	
'HI7e'		Cash	
'AM2a'	Amount type	Purchase	
'AM2b'		Refund	
'AM2c'		Cash	
'AM2d'		Amount	
'AM4'	V.A.T.	VAT incl.	
'AM5'	Surcharge	Surcharge	
'AM6'	Cashback	Cashback	
'AM7' / 'AM11'	Extra	Extra	
'AM9' / 'AM13'	Total	Total	
'TR1'	PIN indicator	PIN used	
'TR3'	Payment code	Paym.code:	
'TR4a'	Account type	Saving transaction	
'TR4b'		Debit transaction	
'TR4c'		Credit transaction	
'TR8'	Merchant number	Me.No:	
'TR12'	Status	Status:	
'TR13'	Auth.code	Auth.code:	
'TR14a'	Auth.result	Authorized	
'TR14b'		Authorized	
'SI2/SI4'	Tips info – 1	** When tipping **	
'SI3/SI5'	Tips info – 2	Ask for new receipt	
'SI6/SI7'a	Approval message	?Approved for \ crediting of account	
'SI6/SI7'b		?Approved for debiting\ of account as above	

Table 1-15.5 - Messages for Printing (reference) (*concluded*)

Receipt Line	Element	English	National
'SI8'	Card reference	Printed digits:	
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	
'SI16'	ID expiry date	ID expiry date:	
'SI18'	Clerk ID	Clerk ID:	
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholder's account by the issuer	
'SI26'a	Signatory type	Merchant's signature	
'SI26'b		Cardholder's signature	
'FI2'a	Termination reason	Interrupted – cancel	
'FI2'b		Declined	
'FI2'c		Signature declined	
'FI2'd		Interrupted – error	
'FI7'		Keep receipt	
'FI8'a	Recipient indicator	Cardholder's receipt	
'FI8'b		Merchant's receipt	
'PC3'	Balance amount	Balance	
'PC4'	Expiry date	Exp. date	
'CL1'	Maximum Deposit	Max Deposit	
'CL2'	Available Funds	Available Funds	
'CL3'	Balance before	Balance before	
'CL4'	Charge of card	Charge of card	
'CL5'	Card balance	Card balance	

This page is intentionally left blank

1-13 Single Unit Terminals

1-13.1 Introduction

An attended terminal may be designed as a Single Unit Terminal (SUT) operated by both the merchant and the cardholder.

When the merchant and the cardholder share the same physical user interface (display and key pad), the transaction sequence must control the security issues concerning PIN-entry on a keyboard which operates in both PIN-Entry mode and Clear-Text mode.

This document defines the requirements for such a terminal configuration.

1-13.2 Conditions and Requirements

To avoid that a cardholder accidentally enters the PIN while the numeric keyboard is in Clear-Text mode, the transaction sequence for merchant and cardholder shall be clearly separated.

The transaction shall be split into 3 sequential steps:

1. Merchant: Sets up the transaction conditions
2. Cardholder: Reads card, enters PIN and accepts amount
3. Merchant: Transaction completion including receipt printing.

The PSAM will issue the Check Stop List command to see if an electronic Stop List is supported by the terminal and to check if the actual card is shown on the list.

- The support of automatic Stop List check may be omitted. If omitted, the terminal shall respond to the Check Stop List command accordingly.

The merchant may force a transaction to be performed offline. In this situation the terminal should ask the merchant whether an Authorization Code has been obtained manually or not (and in case a code is received, enable manual entry of the code).

- The support of Forced Offline may be omitted.
- The support of Forced Offline may be maintained, but the procedures for manual entry of Authorization Code may be omitted by the merchant. If omitted, the terminal shall respond to the *Check Stop List* command accordingly.

- If support of Forced Offline is maintained, and the procedures for manual entry of Authorization Code is maintained too, the merchant shall perform the Voice Authorization Call and enter the code when the PAN is known. This may require that the terminal is handed over temporarily to the merchant after the cardholder has performed Application Selection.
If the Voice Authorization Call is performed before the transaction is initiated, the PAN embossed on the card will be used. But in case of multi-application cards it may be impossible to visually read the PAN of the selected application.

The support of Fallback (from ICC to magnetic stripe) shall be implemented.

When the cardholder is requested to return the terminal to the merchant, the following text message (saying "Hand over the Terminal") shall be displayed (example given for a terminal intended for installation in Denmark):

- "Aflever Terminal"

When the transaction result is available for PIN and No CVM transactions, the terminal shall first display the result to the Cardholder, and (after the the terminal is handed over) then display the result to the merchant. The messages displayed to the Cardholder and to the merchant respectively shall follow the requirements defined in this specification.

When the preliminary transaction result is available for Signature transactions (before the cardholder signs the receipt), the terminal shall be handed over the the merchant and the final part of the transaction processing/flow shall be controlled by the merchant.

Generally, the transaction flow shall be separated in 3 main steps as defined in the table below.

Table 1-13.1 - Transaction Flow

Step	Operator	Functions
1	Merchant	<u>Setup transaction conditions</u> <ul style="list-style-type: none"> – Select Transaction Type (Purchase/Re-fund) – Amount Entry – Select 'Forced Signature' (if relevant) – Select Fallback (if the ICC has failed) – Select 'Forced Offline' (if relevant/implemented) – Optionally select 'Payment Condition Code'
2	Cardholder	<u>Cardholder Card entry, PIN entry and amount acceptance</u> <ul style="list-style-type: none"> – Card Entry (Insert or swipe) – Application Selection – Optionally select 'Account Type' – PIN Entry – Amount Approval – "Wait" while (online) processing is completed – Display result: <ul style="list-style-type: none"> – PIN/No CVM: Display <final result> to the cardholder and "Return Terminal" – Signature: Display "Return Terminal"
3	Merchant	<u>Merchant Transaction completion</u> <ul style="list-style-type: none"> – The merchant continues the flow by activating a 'specific key or function' (implementation dependent). – Print receipt(s) – Accept signature (if required) – Print additional receipt(s). – The <final result> is displayed to the merchant.

1-13.3 Examples

Figures 1-13.1 to 1-13.4 on the following pages depict examples of the general message flow during different types of transactions.

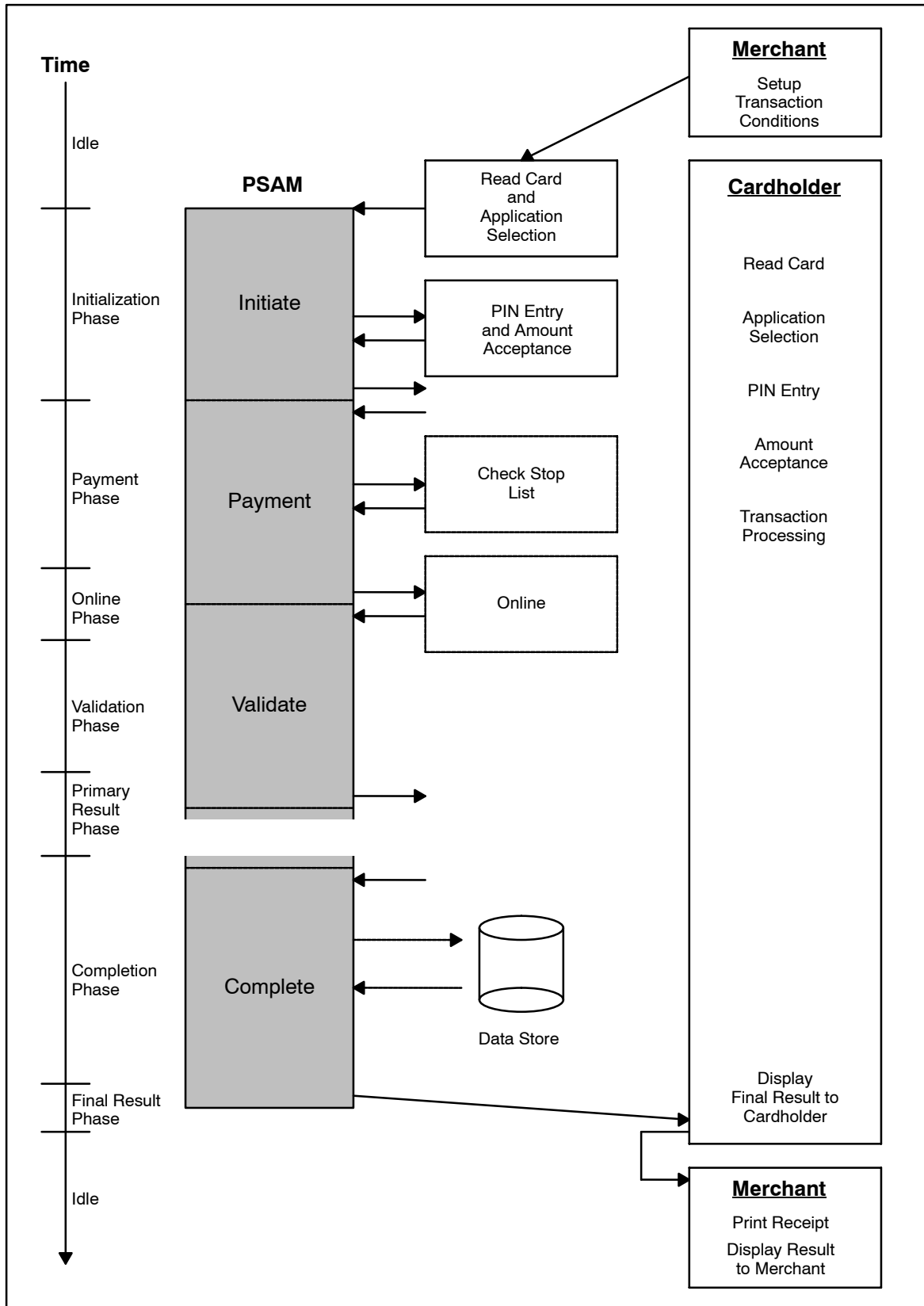


Figure 1-13.1 - PIN Transaction

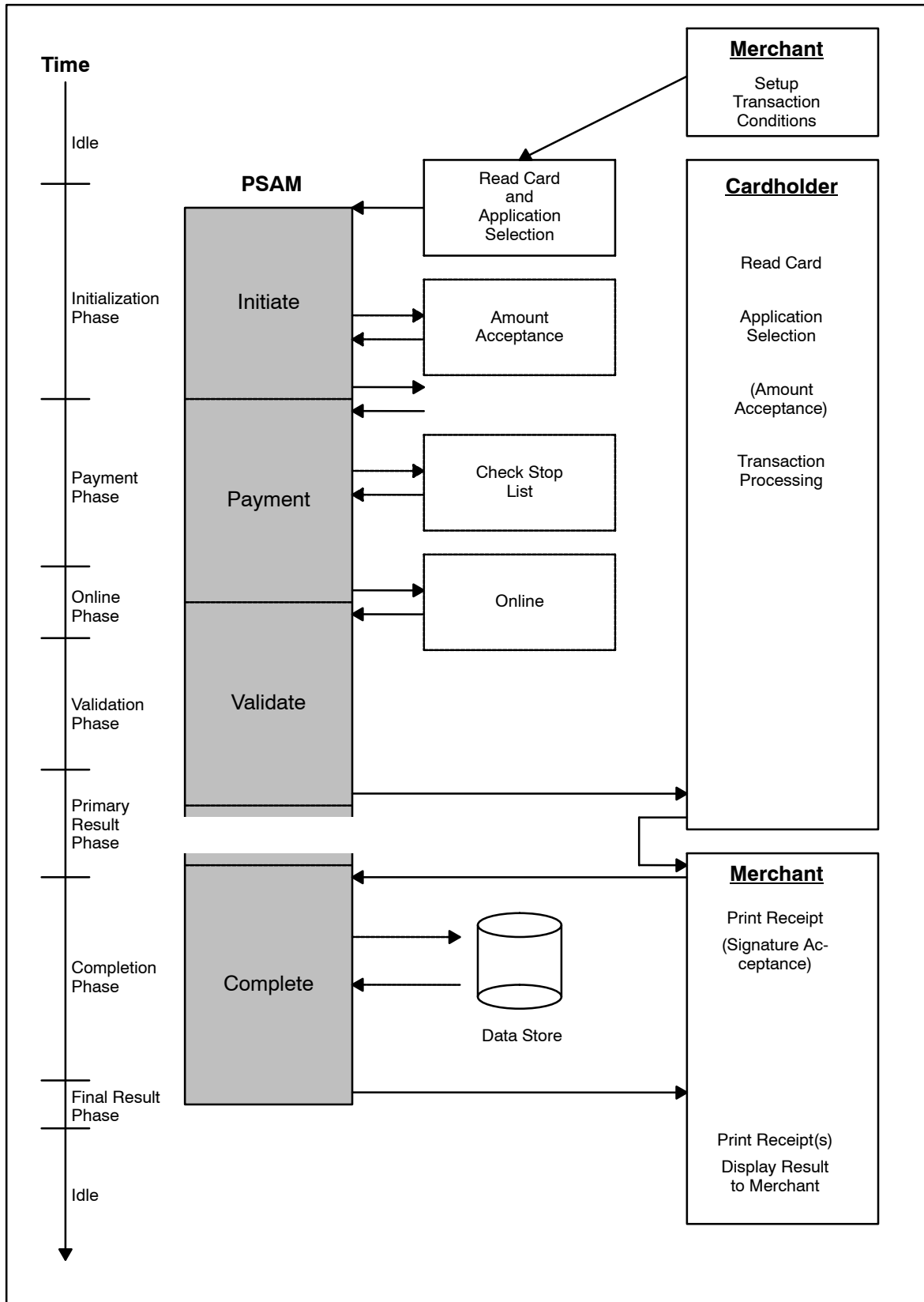


Figure 1-13.2 - Signature Transaction

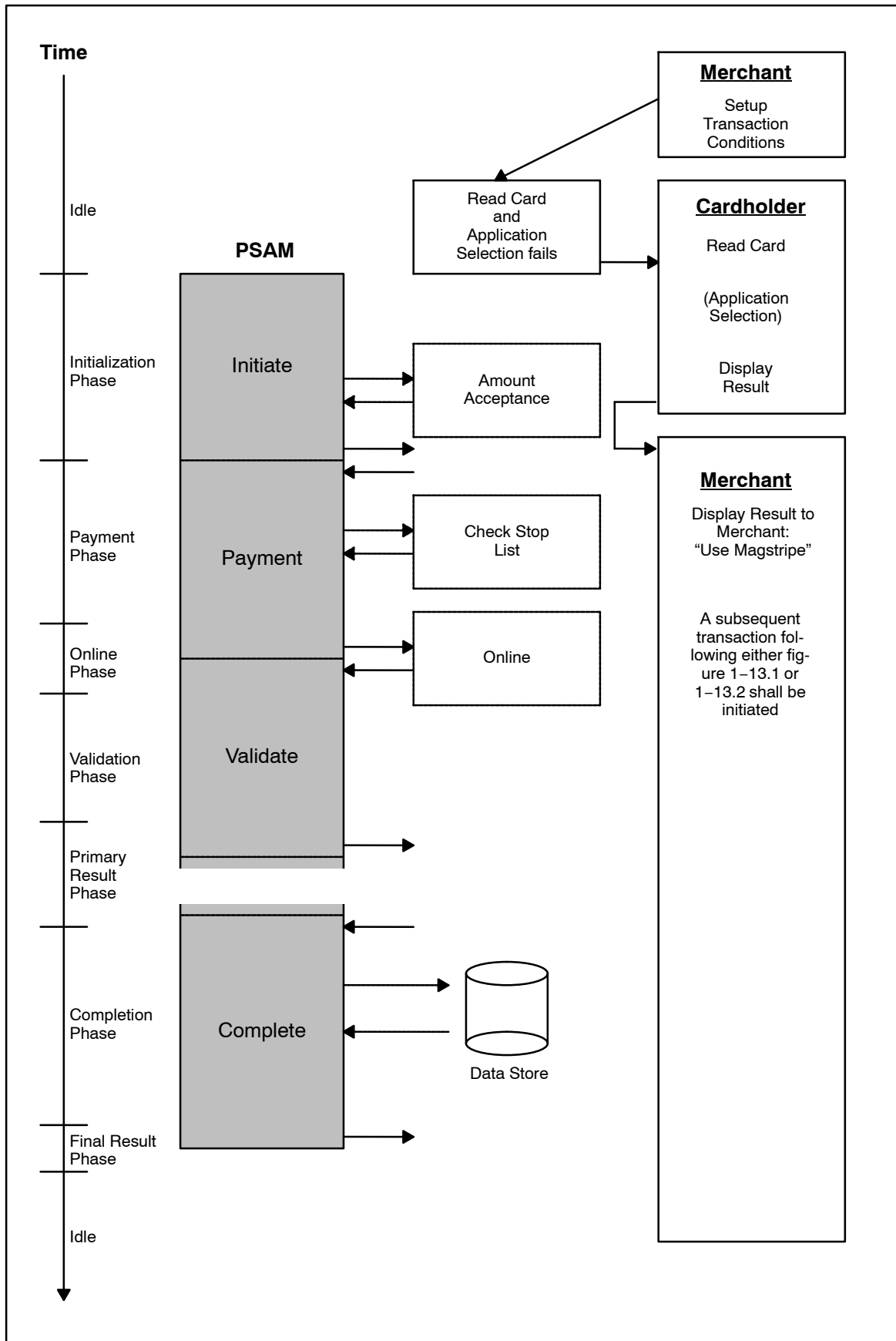


Figure 1-13.3 - Fallback (Noticed before Application Selection is Completed)

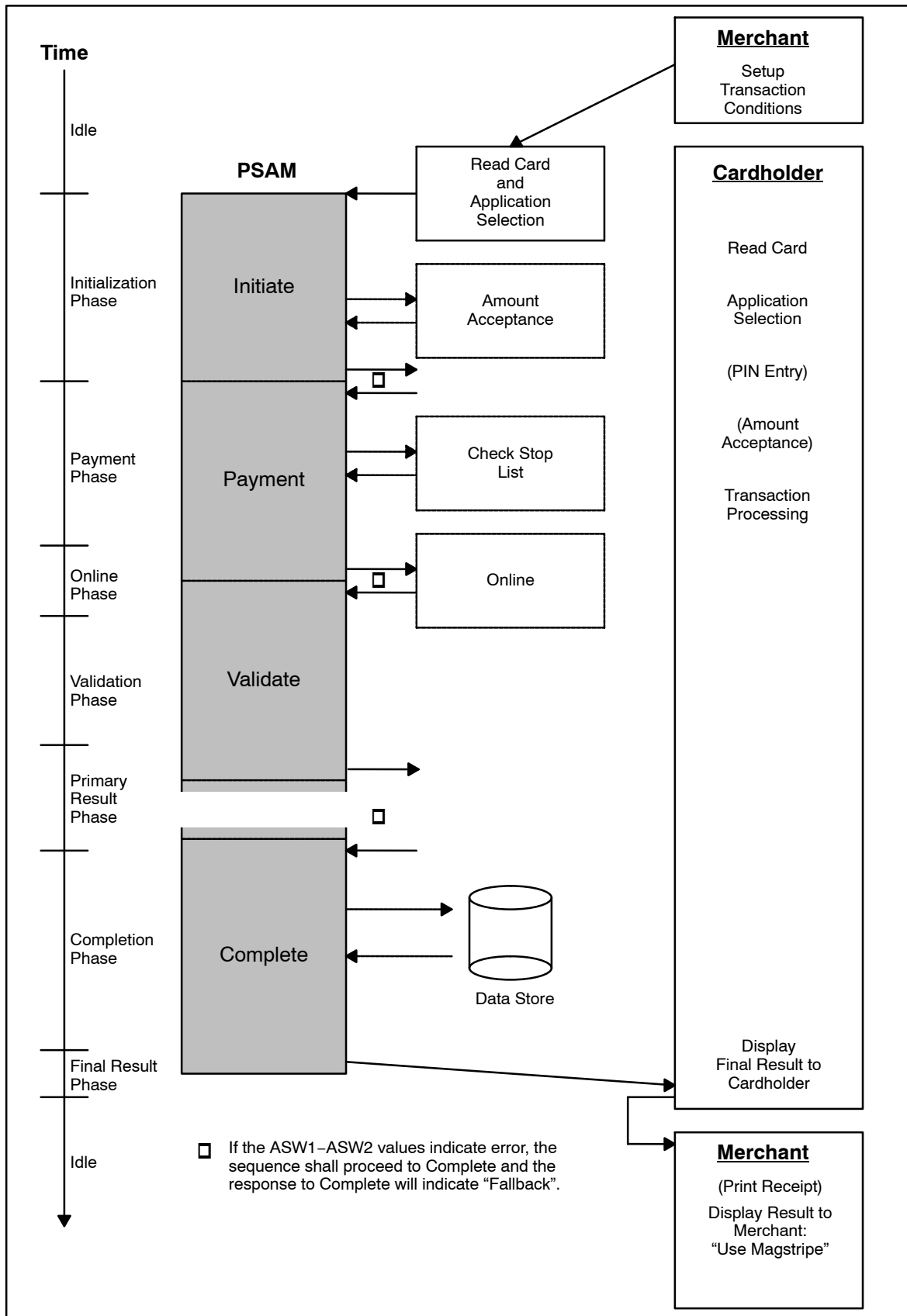


Figure 1-13.4 - Fallback (Noticed after Application Selection is Completed)

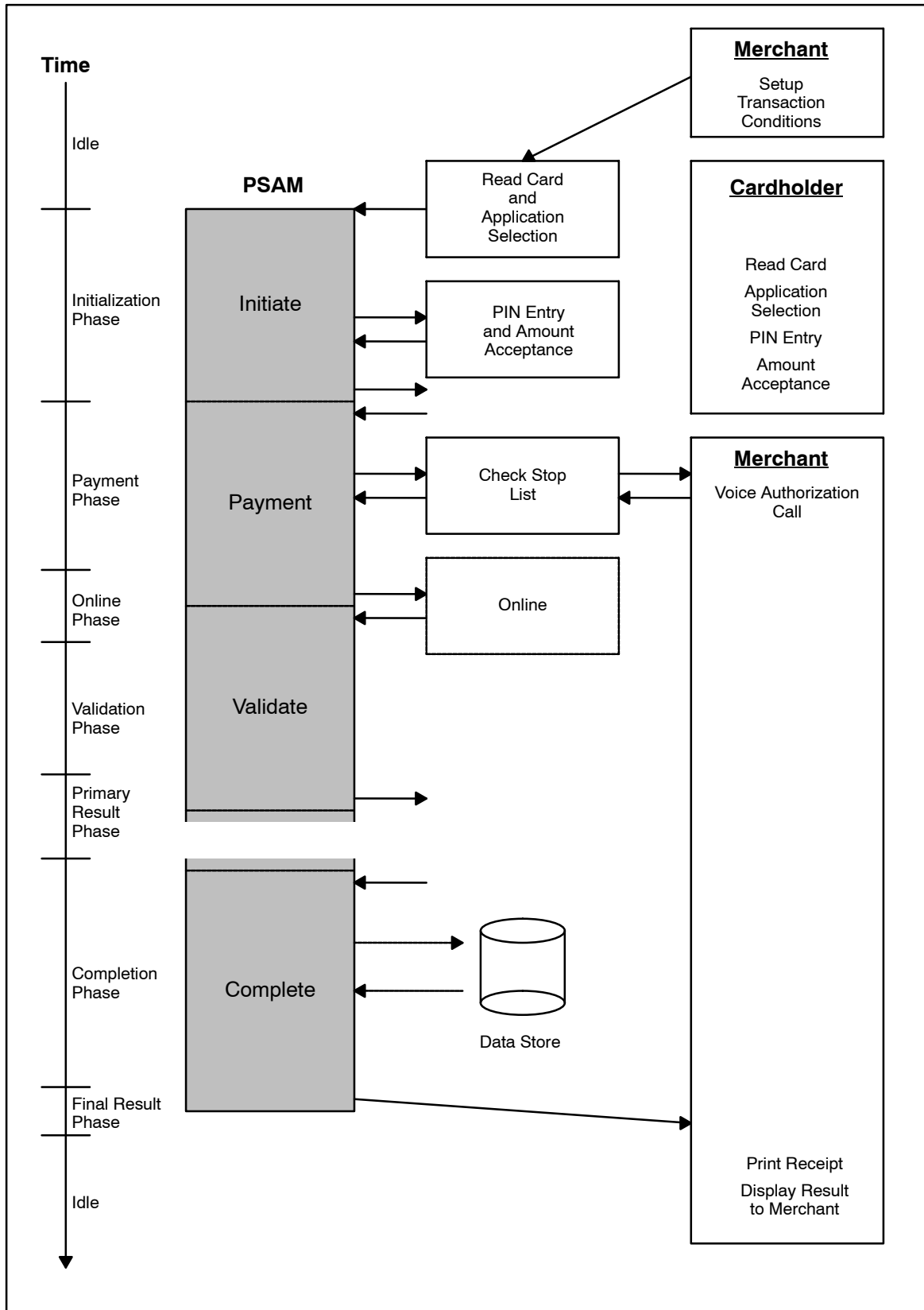


Figure 1-13.5 - PIN Transaction - Forced Offline

NOTE: The Voice Authorization Call is based upon the PAN returned from the PSAM in the *Check Stop List* command.

1-14 Business Requirements

1-14.1 General Requirements

1-14.1.1 Business Calls and Terminal Environments

The defined Business Calls may not be relevant in all terminal environments.

- 1-14.1.1.1 A If the cardholder shall be able to pay for goods, services or cash, the terminal shall support Purchase and/or Capture.
- 1-14.1.1.2 B If the terminal is attended and either Purchase or Capture is supported, the terminal shall support Refund.
- 1-14.1.1.3 A If Capture is supported, Original or Extended Authorization and Reversal (Authorization) shall be supported.
- 1-14.1.1.4 C If Capture is supported, Supplementary Authorization may be supported.
- 1-14.1.1.5 B If the terminal is attended and either Purchase or Capture is supported, the terminal shall for some regions support Cancellation.

1-14.1.2 Terminal Profiles

The Terminal Supplier must decide which functionality should be implemented.

- 1-14.1.2.1 A The terminal shall be capable of handling debit/credit cards
- 1-14.1.2.2 B If debit/credit cards are supported, *both* IC Cards and magnetic stripe cards shall be supported.

- 1-14.1.2.3 A The terminal shall be either:
- Attended, or
 - Unattended (Unattended Payment Terminal, UPT).
- In certain environments, terminals may be attended some of the time, while left unattended the rest of the time.

1-14.2 Application Initialization

1-14.2.1 Power On

- 1-14.2.1.1 A The following data elements:
- Type of application
 - PSAM ID
 - MAD-Handler ID
 - Terminal Software version no. (Build date)
 - EMV Checksum
 - PSAM Code Checksum
 - PSAM Config Checksum
- shall be available for maintenance purposes e.g. printed in a terminal report.
- 1-14.2.1.2 C The data elements listed in requirement 1-14.2.1.1 may be displayed after power-up on the Merchant Display (attended terminal) or the Cardholder Display (unattended terminal).
- NOTE:** The data elements EMV Checksum, PSAM Code Checksum and PSAM Config Checksum shall be obtained from the response to the *Get Debit/Credit Properties* command with identifier '0007'.
- 1-14.2.1.3 B The following data elements (in addition to the data elements listed in requirement 1-14.2.1.1):
- PED info
 - PSAM version
 - PSAM Subversion
 - Service Packs requested
 - Host Interface info (e.g. IP-address, Port no., communication network)
- shall be available for maintenance purposes e.g. printed in a terminal report.
- 1-14.2.1.4 C The data elements listed in requirement 1-14.2.1.3 may be displayed after power-up on the Merchant Display (attended terminal) or the Cardholder Display (unattended terminal).

1-14.3 Application Selection

1-14.3.1 Introduction

Preparation

When a card has been read by one of the card readers, the terminal must decide if an application in the terminal as well as in one or more of the PSAMs can perform transactions with the actual card.

NOTE: Some applications support only ICCs *or* MSCs where others support both.

Similar for both card types is the initial preparation of tables to perform the application selection at transaction time for each card presented. At the very first terminal initialization, the terminal requests a table for MSC selection and a table for ICC selection from each relevant application and/or PSAM present in the terminal.

NOTE: During normal operation, a PSAM may indicate to the MAD-Handler that new data has been received. The MAD-Handler must then request the selection tables again from that PSAM.

Magnetic Stripe Cards (MSCs)

For magnetic stripe cards, the decision whether the card can be handled is fairly simple, as the only parameter for this decision is the contents of the magnetic stripe. More precisely, the first (1 to 8) digits, also called the prefix, of the PAN (Primary Account Number).

Integrated Circuit Cards (ICCs)

For ICCs, the decision may be more complex, as the card may support several applications, of which the terminal (MAD-Handler and PSAM) may only support some. Therefore, application selection may also comprise a dialogue with the cardholder to select which application from the mutually supported ones (also named Candidate List) should be used.

1-14.3.2 Building the MSC Selection Table

The MSC Selection Table consists of a number of MSC Selection Records, each associated with the recognition and handling of a specific card type.

Some card schemes can be represented by a single entry in the MSC Selection Table. E.g. the cards from a local supermarket chain which only issues cards where the PANs begin with 567890.

Other card schemes (especially worldwide schemes with many participating issuers) may require a few or several en-

tries. An example is the Danish debit card “Dankort” which is also available for international use (“VisaDankort”).

To identify a “Dankort” when used domestically, two entries are required in the MSC Selection Table: 4571xxxx and 5019xxxx.

NOTE: Applications not using a PSAM shall insert their entries in the selection table according to the requirements defined below.

- 1-14.3.2.1 A For each application supporting MSCs, the terminal shall obtain the prefixes supported by the individual applications.

NOTE: The terminal uses the *Get MSC Table* command to each corresponding PSAM application that has successfully performed the *Start-up PSAM* command for obtaining the prefixes supported by the individual PSAMs. The response to the *Get MSC Table* command contains all PAN ranges supported by that PSAM application.

- 1-14.3.2.2 A The terminal may have a MSC application able to handle PAN ranges outside the PSAM'. The application shall not process such transaction unless the range is enabled in the MSC selection table.

NOTE: The PSAM delivers information on PAN ranges the terminal may support in the data element Card Service Info in the response to *Get Debit/Credit Properties, Additional MSC Info*. See section 1-10.4 for further details.

NOTE: A PAN range may be enable for processing outside the PSAM, and at the same time processed by the PSAM. An example of this could be a Private Label Card, where the transaction is processed by Nets, but bonus information handled outside the PSAM.

- 1-14.3.2.3 A The terminal shall store a record for each PAN range.

NOTE: Other implementations, e.g. relational data bases are allowed if the functionality defined here is complied with.

An example of an MSC Selection Record is given in Table 1-14.1.

Table 1-14.1 - MSC Selection Record (Example)

Data element	Value	Length
PAN _{FROM}	PAN range from	4
PAN _{TO}	PAN range to	4
ID _{PSAMAPP,N}	TAPA application ID	1)
Pointer to the PSAM	Unique pointer to the PSAM supporting the ID _{PSAMAPP} listed above	1)
DD	Discretionary Data	1)
NOTES:		
1) Implementation dependent.		

- 1-14.3.2.4 A Each MSC Selection Record record shall at least contain the PAN_{FROM} and PAN_{TO} data elements and a value that identifies either the application or, where PSAMs are concerned ,both the PSAM Identification and ID_{PSAMAPP}.
- 1-14.3.2.5 C Discretionary Data (DD) may be added to each MSC Selection Record as needed by the terminal.
- NOTE:** The prefix 4571xxxx used in the example above is indicated by the PSAM by setting PAN_{FROM}= '45710000' and PSAM_{TO}= '45719999'.
- NOTE:** The value identifying the PSAM as well as the PSAM application may be a short pointer to a translation table to save space. Alternatively, the full data elements (PSAM Identification and ID_{PSAMAPP}) may be stored.
- NOTE:** More than one PSAM may support a given PAN range, e.g. if two Nets PSAMs are present for load sharing purposes in a terminal with several card readers.
- 1-14.3.2.6 A When storing entries from a given PSAM or application, the terminal shall make sure that no previous records for the same PSAM/application are present in the MSC Selection Table, e.g. by actively deleting old entries before requesting new ones.
- 1-14.3.2.7 C The MSC Selection Table should be kept in non-volatile memory to avoid the need for rebuilding it after power-up.
- 1-14.3.2.8 A The terminal shall, for each PSAM ID supported, retain up to 254 records in the MSC Selection Table.
- NOTE:** The total size may depend on other applications (and possible PSAMs) not defined by Nets Denmark A/S.
- Depending on the algorithm chosen for using the tables, they may need sorting after having obtained information from all the applications and all the installed PSAMs. This is especially relevant when a terminal supports both (local) applications and one or more PSAM applications.

1-14.3.3 Building the AID Selection Table (for ICCs)

The AID Selection Table consists of a number of AID Selection Records each associated with the recognition and handling of a specific card type.

Most card schemes can be represented by a single entry in the AID Selection Table.

As for MSCs, some card schemes may require a few entries.

- 1-14.3.3.1 A For each application supporting ICCs, the terminal shall obtain the AIDs supported by the individual applications.
- NOTE:** The terminal uses the *Get Supported AIDs* command to each corresponding PSAM application that

has successfully performed the *Start-up PSAM* command for obtaining the AIDs supported by the individual PSAMs. The response to the *Get Supported AIDs* command contains all AIDs supported by that PSAM application.

NOTE: The order in which the AIDs appear in the response does not indicate any priority.

- 1-14.3.3.2 A The terminal shall, if it has an ICC application able to handle AIDs not supported by a PSAM, ensure that all AIDs supported by a PSAM always are handled by a PSAM.

NOTE: Using an application handling AIDs not supported by the PSAM may enforce PCI requirements on the system.

- 1-14.3.3.3 A The terminal shall store a record for each AID.

NOTE: Other implementations, e.g. relational data bases are allowed if the functionality defined here is complied with.

An example of contents in an AID Selection Record is given in Table 1-14.2.

Table 1-14.2 - AID Selection Record (Example)

Data element	Value	Tag	Length	Use
LEN _{AID,N}	Length of N'th AID	-	1	Obtained by the <i>Get Supported AIDs</i> command
AID _N	N'th AID	-	5 – 16	
Card Name _N	Default Card Name linked to the N'th AID	'DF70'	16	Obtained by the <i>Get D/C Properties ('0009')</i> command
ASI _N	Application Selection Indicator (N'th AID)	'DF71'	1	
ID _{PSAMAPP,N}	TAPA application ID	-	X ¹⁾	1) Implementation dependent
Pointer to the PSAM	Unique pointer to the PSAM supporting the ID _{PSAMAPP} listed above	-	X ¹⁾	
Card Product Type _N	Indicator for the type of card (N'th AID)	'DF72'	2	Obtained by the <i>Get D/C Properties ('0009')</i> command
Card Product Functions _N	Indicator for the functions available for the card (N'th AID)	'DF73'	4	
Card Product Flow _N	Indicator for the flow defined for the specific functions (N'th AID)	'DF74'	2	Obtained by the <i>Get D/C Properties ('0009')</i> command (Optional)
Card Product EMV Entry Point Parameters _N	Currency Code (N'th AID)	'DF75'	2	
	Currency Exponent (N'th AID)		1	
	Terminal Contactless Floor Limit (N'th AID)		4	
	Terminal Floor Limit (N'th AID)		4	
	Terminal CVM Required Limit (N'th AID)		4	
	Terminal Contactless Transaction Limit (N'th AID)		4	
	Card Product Limit Flags (N'th AID)		1	
	Terminal Transaction Qualifiers (N'th AID)		4	
	Default Contactless Application Capabilities (N'th AID)		8	
Terminal Decision Flags _N	Internal flags for N'th AID		1	Internal flags reset/set during Pre-processing according to ref. 21. "Entry Point Specification"
Copy of Terminal Transaction Qualifiers _N	Internal data element for N'th AID		4	To be forwarded to the PSAM

Legend: Grey rows indicates additional data elements required when Prepaid ICC is supported.

1-14.3.3.4 A Each AID Selection Record shall at least contain:

- the AID (including length information)
- ASI (Application Selection Indicator)
- a value that identifies either the application or, where PSAMs are concerned, both the PSAM Identification and ID_{PSAMAPP}.
- Card Product Type
- Card Product Functions

- 1-14.3.3.5 C For each AID received in the response to the *Get Supported AIDs* command the MAD-Handler may link the corresponding Card Name.

NOTE: The corresponding Card Names may be taken from the response to the *Get Debit/Credit Properties* commands (Identifier = '0009') issued to a PSAM for each AID supported by that PSAM in the AID Selection Table.

NOTE: If the terminal does not link the corresponding Card Names, the terminal may acquire the relevant Card Name “on the fly” during the application selection.

- 1-14.3.3.6 A For each AID received in the response to the *Get Supported AIDs* command, the terminal shall assign the value for the corresponding ASI (Application Selection Indicator).

NOTE: The value assigned for the ASI is taken from the response to the *Get Debit/Credit Properties* commands issued to a PSAM for each AID supported by that PSAM in the AID Selection Table.

- 1-14.3.3.7 A If the data element Card Product Functions is not available in the *Get Debit/Credit Properties* commands (Identifier = '0009') response, the terminal shall set the default value of 'FF 00 00 00' (Debit/Credit enabled).

When using the *Get Debit/Credit Properties* command for retrieving the ASI, Card Name, Card Product Type and Card Product Functions, the Identifier shall be '0009' and the Additional Info field shall contain the AID previously received in the response to the *Get Supported AIDs* command as input data.

The *Get Debit/Credit Properties* command with an identifier in the range '0001' - '0008' can be issued at any time after the Answer-to-Reset has been received from the PSAM.

NOTE: In case of an erroneous response (data not available, syntax error etc.), the ASW1-ASW2 will be in the range '10XX'.

An example of how the AID Selection Record can be build is given in figure 1-14.1.

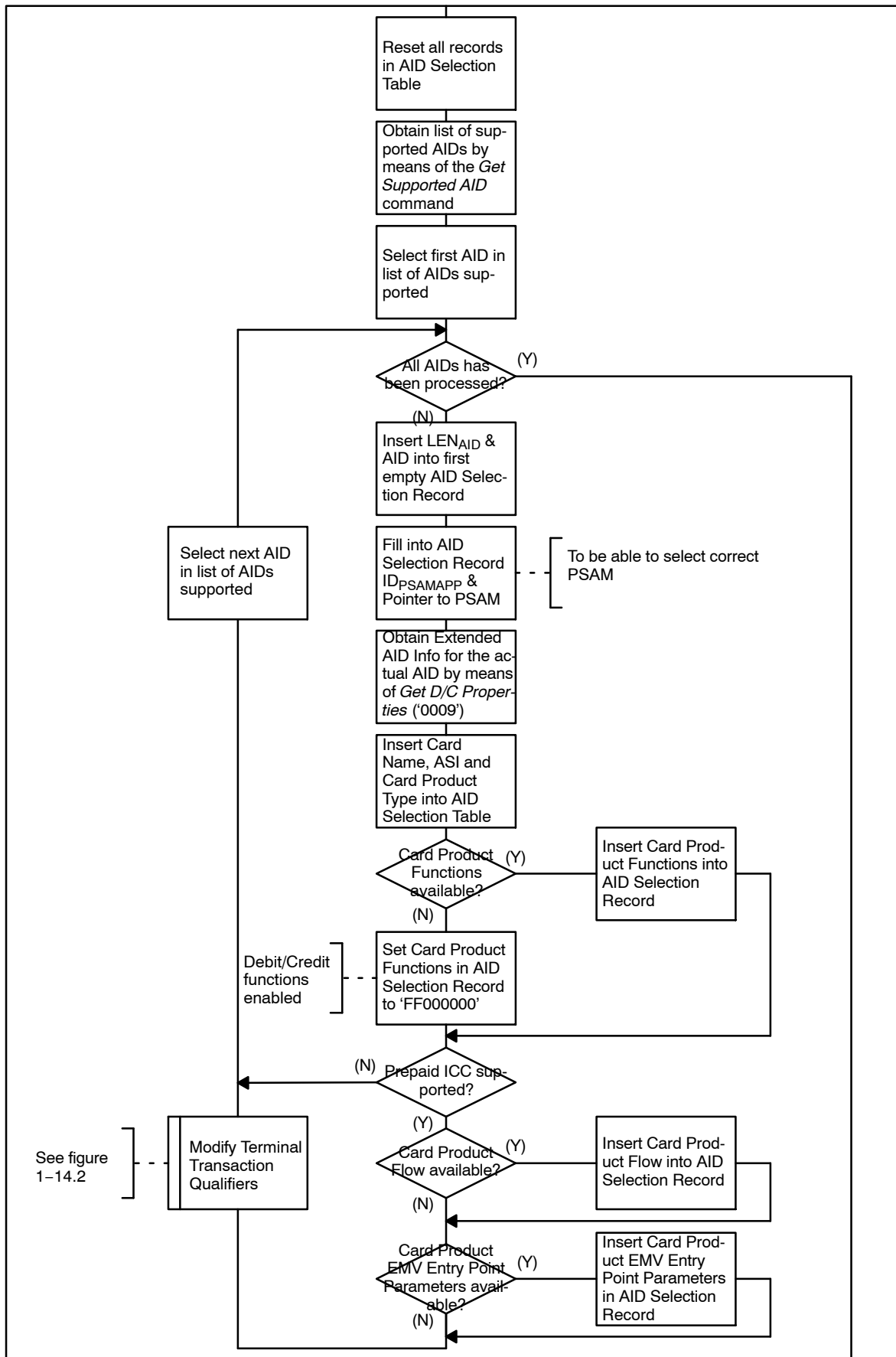


Figure 1-14.1 - Build AID Selection Record

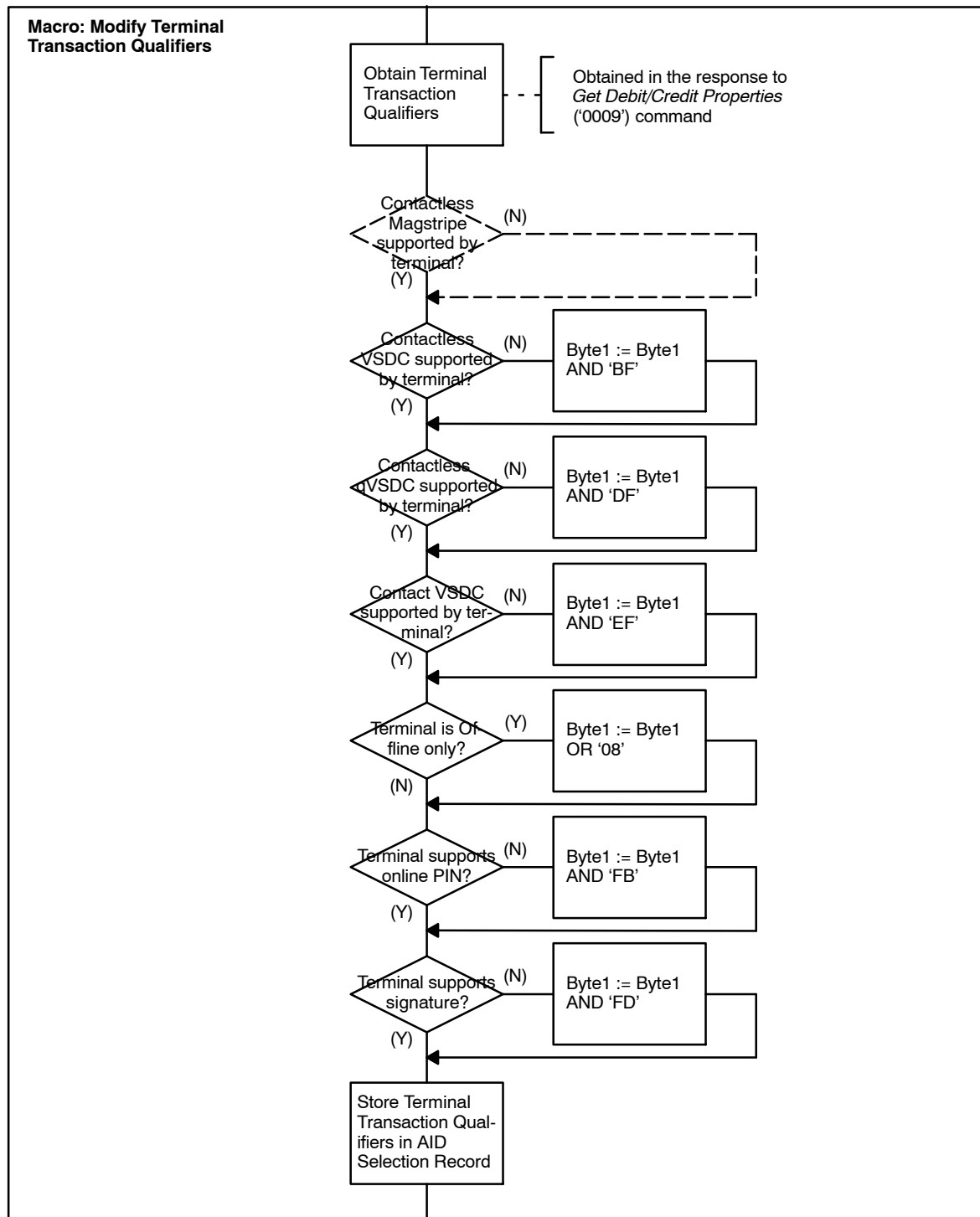


Figure 1-14.2 - Macro: Modify Terminal Transaction Qualifiers

Discretionary Data

1-14.3.3.8 C Discretionary Data (DD) may be added to each AID Selection Record as needed by the MAD-Handler.

NOTE: The value identifying the PSAM as well as the PSAM application may be a short pointer to a translation table to save space. Alternatively, the full data ele-

ments (PSAM Identification and $ID_{PSAMAPP}$ may be stored).

NOTE: More than one PSAM may support a given AID, e.g. if two PSAMs are present for load sharing purposes in a terminal with several card readers.

- 1-14.3.3.9 A When storing entries from a given PSAM, the terminal shall make sure that no previous records for the same PSAM application are present in the AID Selection Table, e.g. by actively deleting old entries before requesting new ones.
- 1-14.3.3.10 C The AID Selection Table should be kept in non-volatile memory to avoid the need for rebuilding it at each power-up.
- 1-14.3.3.11 A The terminal shall be capable of storing up to 100 records in the AID Selection Table.

NOTE: The total size may depend on other applications (and PSAMs) not defined by Nets Denmark A/S.

1-14.3.4 MSC Application Selection

When an MSC has been read, the terminal shall find the best match between the PAN from the magnetic stripe and the entries in the MSC Selection Table.

No dialogue with the cardholder is needed for this as the MSC only contains a single “application”.

The object for the MAD-Handler is to find the most “narrowly” defined MSC Selection Record where the PAN read from the MSC is included. To make this decision, the following term will be used:

PAN range width, the number of prefixes included in the range, i.e. $PAN_{TO} - PAN_{FROM} + 1$. The subtraction shall be performed on the decimal value after unpacking the BCD values.

Two different approaches are described below. The general requirements are defined before describing the two methods.

Other implementations are, however, allowed if the same functionality is obtained.

- 1-14.3.4.1 A The application selection mechanism for MSCs shall be based on the MSC Selection Table.
- 1-14.3.4.2 A If the MSC PAN is only included in one MSC Selection Record, MSC application selection is considered successful and the MAD-Handler and PSAM applications indicated by that record shall be used.
- 1-14.3.4.3 A If the MSC PAN is included in more MSC Selection Records with *identical* PAN range widths, the MAD-Handler may select freely (or using criteria's outside the scope of this specification) between the terminal and PSAM applications pointed at from those records.

- 1-14.3.4.4 A If the MSC PAN is included in more MSC Selection Records with *different* PAN range widths, the terminal shall select the record with the smallest PAN range width (the most precisely defined prefix).
- 1-14.3.4.5 A If the MSC PAN is not included in any of the MSC Selection Records, MSC application selection is considered unsuccessful and the Cardholder Display shall display the message code '0C' ("Not accepted").
- 1-14.3.4.6 A Only the first 8 digits of the PAN shall decide whether the PSAM supports the actual PAN.

NOTE: See section 2-4.7.2 for further requirements concerning the validation performed by the terminal.

Searching an Unsorted MSC Selection Table

The terminal must search all MSC Selection Records and save the first record where the MSC PAN is included. The search must continue and if another match occurs, the MSC Selection Record with the smallest PAN range width shall be saved as the new preliminary match. When the entire table has been searched, the match (if any) is used. Criteria's to choose between two records with identical PAN range widths are outside the scope of this specification.

Searching a Sorted MSC Selection Table

To speed up MSC application selection, the terminal may sort the MSC Selection Table according to PAN range widths. By starting the search at the MSC Selection Record with the smallest PAN range width, the first record where the MSC PAN is included is the final selection, i.e. the search can stop. Criteria's for ordering records with identical PAN range widths are outside the scope of this specification.

NOTE: The MSC selection table supplied from Nets Denmark A/S will be supplied with most narrow PAN range first.

1-14.3.5 ICC Application Selection

When an ICC has been inserted in the ICCR, the terminal must perform application selection before proceeding to the actual transaction processing.

Applications are identified using the Application Identifier (AID), e.g. the Dankort is identified by one AID and Visa/Dankort is identified by another AID.

Application selection is performed by the terminal by matching the AIDs supported by the terminal and the AIDs supported by the ICC. If more matches exist, the cardholder must select between the mutually supported applications (Candidate List).

NOTE: Some AIDs can share the same terminal/PSAM application, e.g. the AIDs for "Dankort" and "Visa/Dankort".

- 1-14.3.5.1 A ICC Application selection shall be performed according to ref. 20: "EMV ICC Specification".

Candidate List

The terminal may use the "Payment Systems Directories" in the ICC (if present) or shall at least support the "AID List" (the AID Selection Table) for building the Candidate List as defined in ref. 20: "EMV ICC Specification".

- 1-14.3.5.2 B The terminal shall be able to handle a Candidate List containing at least 10 entries.
- 1-14.3.5.3 B If there is no priority sequence specified in the card, the list shall be in the order in which the applications were encountered in the card.
- 1-14.3.5.4 A If an AID supported by the ICC matches an AID Selection Record, then the AID shall be included in the Candidate List.
- 1-14.3.5.5 A The terminal shall use the ASI to determine whether exact match between the ADF name in the card and the AID in the terminal is required or partial match is allowed. See ref. 20: "EMV ICC Specification".

NOTE: The value assigned for the ASI is taken from AID Selection Table or the response to the *Get Debit/Credit Properties* commands issued for the AID.

NOTE: The format of the ASI can be found in section 2-15, "Data Elements".

- 1-14.3.5.6 A The AIDs supported by the ICC shall be checked against all the AID Selection Records to find *all* possible matches.
- NOTE:** If the terminal only supports a few AIDs, it may be more efficient to issue a number of *Select* commands according to ref. 20: "EMV ICC Specification" for these particular AIDs.

- 1-14.3.5.7 A If a match is identified between an AID supported by the ICC and more than one AID Selection Records, then the AID Selection Record with the largest number of digits for the AID ($LEN_{AID,N}$) shall be accepted as the only one.

- 1-14.3.5.8 A If a match is identified between an AID supported by the ICC and more AID Selection Records with the same number of digits defined ($LEN_{AID,N}$), then the terminal shall select one of the AID Selection Records.

NOTE: The terminal may use any criteria for this selection.

- 1-14.3.5.9 B If the terminal supports PIN, the terminal shall offer the cardholder the ability to choose the application to be selected, if the actual Candidate List includes more than one AID and the transaction is not a Refund.

NOTE: When displaying the Candidate List requirement 1-14.3.5.13 shall be observed.

- 1-14.3.5.10 B If the terminal supports PIN, the terminal shall offer the cardholder the ability to confirm a selection, if indicated by the data element Application Priority Indicator and the transaction is not a Refund.
- NOTE:** Even though the Candidate List includes only one AID, the terminal must display this application and await acceptance by the cardholder.
- 1-14.3.5.11 B If the terminal offers the cardholder the ability to choose the application, the terminal shall also offer the cardholder the ability to confirm a selection.
- 1-14.3.5.12 B During a Refund transaction, the terminal shall offer either the merchant or the cardholder the ability to choose the application to be selected if the actual Candidate List includes more than one AID.
- NOTE:** Application Selection performed by the merchant has priority, but the selection procedure may alternatively be done by the cardholder.

Display Rules

- 1-14.3.5.13 A For mutually supported AIDs, the Card Name shall be displayed according to the following prioritized order:
1. the Application Preferred Name (Tag '9F12'), if present and if the Issuer Code Table Index (Tag '9F11') indicating the part of ISO/IEC 8859 to use is present and supported by the terminal (as indicated in Additional Terminal Capabilities).
 2. the Application Label (Tag '50'), if present, by using the common character set of ISO/IEC 8859.
 3. the Card Name retrieved by the *Get Debit/Credit Properties* command (Identifier = '0009').
- 1-14.3.5.14 A When the final selection is issued the name of the selected application shall be displayed, at least until any cardholder action is requested (e.g. entering of PIN) according to ref. 20: "EMV ICC Specification".
- NOTE:** Even if the terminal and ICC have only one mutually supported AID and Bit 8 of the Application Priority Indicator indicates *no* Cardholder Confirmation, requirement 1-14.3.5.14 apply.
- 1-14.3.5.15 A If none of the AIDs supported by the ICC are supported by any of the PSAMs or applications, the message code '12' ("Use MAG Stripe") shall be displayed on the Cardholder Display in order to initiate a MSC transaction.

1-14.3.6 Combined MSC and ICC Application Selection

Cards may be issued with both a magnetic stripe and an ICC. The magnetic stripe on such a 'hybrid card' may either be:

- a fallback for an application in the ICC or
- an independent application, not matching an ICC application.

The handling of Fallback, i.e. the magnetic stripe is used as back-up for an application in the ICC, is described in section 2-4.17 page 2-4-24.

A combined reader may perform the MSC reading and ICC communication in different orders:

- A combined reader may have read the MSC data before the ICC is in the correct position for ICC communication. Therefore the MSC data is available when the ICC application selection starts. In the following context this type of combined reader is identified as 'MSC read before ICC'.
- A combined reader may read the MSC data after the ICC communication is completed. Therefore the MSC data is not available (and a MSC application will not be identified/recognized) during the ICC application selection process. In the following context this type of combined reader is identified as 'ICC read before MSC'.

Combined readers with 'ICC read before MSC' will not be able to support 'Combined MSC and ICC Application Selection'.

For terminals equipped with a combined reader and supporting "Combined MSC and ICC Application Selection", the following requirements apply:

- | | | |
|------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-14.3.6.1 | C | If no matching ICC applications are identified (i.e. only MSC application is matching) the application selection and transaction flow shall comply with the requirements for 'MSC only'. |
| 1-14.3.6.2 | C | If no matching MSC application is identified (i.e. only ICC applications are matching) the application selection and transaction flow shall comply with the requirements for 'ICC only'. |

Additional information concerning Combined Application Selection may be found in section 2-4.17 page 2-4-24, Fallback from Chip (ICC) to Magnetic Stripe (MSC) where figure 2-4.5 page 2-4-31, Fallback Handling (Combined Readers) and figure 2-4.6 page 2-4-32, Non-Fallback Handling (Combined Readers) show the logical transaction flow.

- | | | |
|------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-14.3.6.3 | C | <p>Combined MSC and ICC Application Selection shall be performed if:</p> <ul style="list-style-type: none"> • a combined reader is used and • a matching MSC PAN is recognized and • the Service Code in the MSC is neither '2xx' nor '6xx' and • one or more matching ICC applications are identified and included in the Candidate List. |
|------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

NOTE: The Service Code from the MSC may be retained by issuing the *Get Debit/Credit Properties* command to the supporting PSAM with the Identifier equal to '0012'.

- 1-14.3.6.4 C When Combined MSC and ICC Application Selection is performed, the MSC application shall be added to the Candidate List on equal terms as the ICC applications.
- NOTE:** The Candidate List of ICC applications shall be built according to the requirements stated for 'ICC only' in section 1-14.3.5 page 1-14-12.
- NOTE:** The Card Name for the MSC may be retained by issuing the *Get Debit/Credit Properties* command to the supporting PSAM with the Identifier equal to '0012'.
- 1-14.3.6.5 C When a MSC application shall be added to the Candidate List, a "pseudo" Application Priority Indicator shall be assigned, with the value B'0xxx1111.
- NOTE:** The value B'0xxx1111 indicates that:
- the MSC application may be selected without confirmation (only relevant if no ICC applications have been added to the Candidate List), and
 - the MSC application is assigned the lowest priority.
- 1-14.3.6.6 C If the Candidate List includes both matching AIDs and a matching MSC PAN, the terminal shall offer the cardholder the ability to choose the application to be selected.

1-14.4 Addendum Records

1-14.4.1 Conditions

The Addendum Record must succeed immediately after the financial transaction when delivered from the Acquirer. In a multi-entry environment, other financial transactions may be concluded before the Addendum Record is available.

1-14.5 Terminal Handlers

1-14.5.1 The Router, Exception Handling

- 1-14.5.1.1 B The Router shall be able to resolve dead-lock situations, e.g. by implementing overall time-out mechanisms.

1-14.5.2 The MAD-Handler, Exception Handling

Regardless of whether the hardware design is a dedicated terminal or the functions are integral parts of a system, the individual components, e.g. modem and printer may fail.

- Error situations may arise during normal operation, due to mains power supply or communication network drop-outs.
- 1-14.5.2.1 A Error situations shall be identified and dealt with by the MAD-Handler.
- Such situations shall be dealt with by the MAD-Handler, either for the purpose of registration if the situation was overcome, or by preventing further operation until the error condition has been corrected.
- 1-14.5.2.2 A If a failure is detected in any of the components, the terminal shall end normal operation and, if possible, display the relevant error-message.
- 1-14.5.2.3 A If the design of the terminal is based on individual components, which may either be switched off, disconnected, disabled or in any other way manually be taken out of operation, then the MAD-Handler shall be able to detect the missing function, and end normal operation, if needed.
- 1-14.5.2.4 A The MAD-Handler shall be able to detect 'Out of Paper' in the receipt printer.
- 1-14.5.2.5 B The MAD-Handler shall be able to detect 'Paper Low' in the receipt printer.
- 1-14.5.2.6 C If 'Paper Low' is detected, the normal <Idle Prompt> on the Merchant Display (if any) shall be replaced by an error-message indicating "Paper low".
- 1-14.5.2.7 A The MAD-Handler shall be able to detect that a power failure has occurred during processing of a transaction.
- 1-14.5.2.8 A When a power-failure has been detected, the CAD shall be able to either complete the operation or ensure that no erroneous data is registered or stored.
- 1-14.5.2.9 A When there is a failure in the receipt printer, an error message on the Cardholder Display indicating that a receipt cannot be printed shall be displayed, see table 1-11.1 page 1-11-2, Message Code 'E1'.

1-14.5.3 The Card Handler, General Requirements

- 1-14.5.3.1 C If any of the card readers are motorized, the card may be retained upon request from the card issuer (via the MAD-Handler/PSAM).
- 1-14.5.3.2 B If any of the card readers are motorized, the card reader shall be a combined reader, i.e. it shall be able to both read the magnetic stripe as well as interface the IC on a card inserted into the card reader.
- 1-14.5.3.3 A If the terminal has a motorized or locking card reader, a mechanism to return the card shall exist, e.g. in the event of a power failure. This mechanism could be a button for the cardholder to activate or could be implemented in a way that cards are automatically ejected when the terminal loses power.

1-14.5.4 User Interface Handler, PIN Pad

Introduction

- 1-14.5.4.1 A The PIN Pad shall fulfil all PIN Pad related requirements defined in ref. 27: "TAPA, Application Architecture Specification".

Additional functional requirements are defined below.

A number of design requirements defined in chapter 2-6 must be fulfilled as well.

See also chapter 1-7 page 1-7-1, Payment Card Industry - Data Security Standard.

- 1-14.5.4.2 A The procedures for security evaluation and audit of key loading as defined by Nets Denmark A/S shall be fulfilled.

Definitions

A **Physically Secure Device** is a hardware device which cannot be successfully penetrated to disclose all or part of any cryptographic key or PIN resident within the device.

A **Secure Cryptographic Device** is a Physically Secure Device, i.e. a physically and logically protected hardware device that provides a secure set of cryptographic services.

Physical and Logical Security

- 1-14.5.4.3 A All systems and equipment shall comply with the requirements for PIN management and security as defined in ref. 13: "ISO 9564-1", Banking - Personal Identification Number management and security.
- 1-14.5.4.4 A Penetration of the PIN Pad shall cause the automatic and immediate erasure of all PINs, cryptographic keys and all useful residue of PINs and keys contained within the device.
- 1-14.5.4.5 A Transmission of the plaintext PIN from the PIN Pad keyboard to the processor where it will be enciphered shall take place within the physical boundaries of the PIN Pad.
- 1-14.5.4.6 A All internal circuits and connections within the PIN Pad shall be highly physically protected and thereby prohibit tapping.
- 1-14.5.4.7 A The PIN Pad shall resist state-of-the-art attacks, such as Static and Differential Power Analysis (SPA/DPA), Bellcore attacks and Timing attacks.
- 1-14.5.4.8 A The PIN shall be enciphered within the Secure Cryptographic Device immediately after the ENTER key has been pressed.

NOTE: All necessary PIN re-encipherment and PIN block reformatting is handled by the PSAM.

- 1-14.5.4.9 A PIN data shall be deleted when returned in the response to the *Get PIN* command or upon a time-out condition.
- 1-14.5.4.10 A The software shall be designed in such a way that its intended functions cannot be misused or circumvented from the outside world.

- 1-14.5.4.11 A The PIN Pad shall not be operational until the PIN Pad ID and related keys have been loaded.

Packaging

- 1-14.5.4.12 A As defined in ref. 27: "TAPA, Application Architecture Specification", the PIN Pad shall be part of a Secure Device, also housing the ICCR and the Cardholder Display.
- 1-14.5.4.13 B The Secure Device shall house the full terminal implementation.

PIN Pad Keyboard

- 1-14.5.4.14 A The PIN Pad shall contain a key for each of the 10 possible PIN digits (0-9).
- 1-14.5.4.15 A The relationship between the numeric value of a PIN digit and the internal coding of that value prior to any encipherment shall be as specified in table 1-14.3.

Table 1-14.3 - PIN Digit Representation

PIN Digit	Binary Representation
0	B'0000
1	B'0001
2	B'0010
3	B'0011
4	B'0100
5	B'0101
6	B'0110
7	B'0111
8	B'1000
9	B'1001

NOTE: It is recognized that alphabetic characters, although not assigned in ref. 13: "ISO 9564-1" and ref. 14: "ISO 9564-2", may be used as synonyms for decimal digits. Further guidance is given in ref. 13: "ISO 9564-1", annex F.

- 1-14.5.4.16 A There shall be only one PIN keyboard for entering PIN on the terminal.

PIN Entry including Display and Audio

The introduction of the amount and the PIN are data acquisition operations confirmed by pressing the "Enter" key.

- 1-14.5.4.17 A Any input shall be confirmed by pressing the validation key "Enter".
- 1-14.5.4.18 A There shall be a separate command key to cancel or correct the PIN entry.

- 1-14.5.4.19 A A visible signal shall indicate data entry and shall be independent of the actual key being pressed.
- 1-14.5.4.20 A A PIN Pad shall support entry of a four (4) to twelve (12) digits PIN.
- 1-14.5.4.21 A Only a fixed symbol, such as the '*' character, shall be displayed for each PIN digit entered.
- 1-14.5.4.22 C A sound (beep or click) may be emitted whenever the a key is pressed. Such sound shall be identical for all 10 PIN keys.
- 1-14.5.4.23 A If the amount is entered on the same key pad as the PIN, the amount shall be validated before PIN entry is allowed.
- 1-14.5.4.24 A The first digit of the PIN to be entered shall be the high-order digit.

Local PIN Verification

Other cards (not acquired by Nets Denmark A/S) with PIN may have the PIN checked by the PSAM/PIN Pad. For more details, see chapter 2-12 page 2-12-1, "Local PIN".

1-14.5.5 User Interface Handler, Cardholder Display

See also section 2-6.2.5 page 2-6-4, Visual Indicators.

General requirements

- 1-14.5.5.1 A The Cardholder Display shall always react on a cardholder action, e.g. when the cardholder presses the Cancel button.
- 1-14.5.5.2 A No display message shall be displayed less than 1 second, e.g. "Wait" shall be displayed for at *least* 1 second even if the event lasts *less* than 1 second.
- 1-14.5.5.3 B If alternating text is used, every sequence of the alternating text shall be displayed for at least 1 second.
- 1-14.5.5.4 B Any text in the display shall be visible at least 3 seconds before the text may be overwritten or deleted, if no legal action by the cardholder has been taken.
- NOTE:** A legal action can be by activating a button or by removing the card. The display can react immediately by clearing the display, clear a line in the display, change part of a text or write a new text.
- 1-14.5.5.5 A Error messages shall be displayed for at least 6 seconds or until the cardholder has performed the appropriate action.
- 1-14.5.5.6 C Essential information, e.g. Amount, may be emphasized on the display, e.g. by using bold characters or a bigger font.

Display texts

- 1-14.5.5.7 A If the Cardholder Display cannot display 4 lines of 20 characters, the display texts shall be edited in cooperation with Nets Denmark A/S.

- 1-14.5.5.8 A If the Cardholder Display supports 4 lines of 20 characters, the display texts shall for English be as stated in table 1-11.1 page 1-11-2. The display texts shall for other languages be as specified in the corresponding tables in the different sections of chapter 1-15.
- 1-14.5.5.9 A The merchant local language shall be supported. The the display texts in the merchants local language are defined in the different sections of chapter 1-15
- 1-14.5.5.10 C Languages other than the merchants local language may be supported.
- 1-14.5.5.11 A If languages other than the merchants local language are supported, English shall be supported as well.

Display requirements

- 1-14.5.5.12 A The display messages shall guide the cardholder through the operational steps of the transaction, e.g. when to insert the card and to the PIN.
- 1-14.5.5.13 B If more than one card is needed to perform a transaction, e.g. a payment card and a loyalty card, the display shall inform the cardholder of the required sequence, if of any importance.

1-14.5.6 Merchant Application Handler, Interface between Terminal and Merchant Application

- 1-14.5.6.1 A The protocol defined for the interface between the terminal and the Merchant Application shall ensure that both parts have a consistent knowledge of the actual transaction step and the final transaction result.
- 1-14.5.6.2 A If the Merchant Application is a separate component e.g. cash register system, the complete solution shall comply to the requirements defined in this document.

NOTE: Reuse of already certified components may make it easier to comply with the requirements, e.g. if the terminal Merchant Application interface includes a software module executed on the cash register system, the interfacing may be simpler.

1-14.5.7 Data Store Handler, General Requirements

- 1-14.5.7.1 A The Data Store defined for storing transactions shall be non-volatile i.e. it shall be able to maintain its contents, even if the terminal is disconnected from the mains power, for a period of 12 months.
- 1-14.5.7.2 B It shall be possible to reset the contents of the Data Store by use of a special service function, e.g. issued from the Merchant Application. This function shall be protected to prevent the merchant from performing this reset (only the Terminal Supplier shall be able to erase the Data Store).

NOTE: Reset of the Data Store is a manufacturer specific function and may, as examples, be protected by a special password/PIN and/or a special card.

NOTE: See section 2-5.15.8 page 2-5-111, Exception Conditions Failed Delivery of Advices

1-14.6 Fallback

1-14.6.1 General Requirements

- 1-14.6.1.1 A If the transaction is aborted due to incorrect handling (e.g. the card has been withdrawn from the card reader before completion of the transaction), chip technology keeps priority and fallback to magnetic stripe shall not be initiated.
- 1-14.6.1.2 A Fallback is not allowed from a non-Debit/Credit application, like a loyalty application, to the Debit/Credit application on the magnetic stripe.

Key Entered Transaction as Fallback

- 1-14.6.1.3 A For EMV cards where the IC is not readable, the fall-back shall be the magnetic stripe if allowed. If the magnetic stripe neither is readable, a key entered transaction may be initiated if allowed.

1-14.7 Cardholder Verification

1-14.7.1 PIN Entry

- 1-14.7.1.1 B The Terminal shall be able to accept PIN as CVM .
- NOTE:** Depending on the environment, unattended terminals may not support PIN.
- 1-14.7.1.2 B The cardholder shall be able to decline a transaction. The terminal shall not start a transaction unless it has been confirmed by the cardholder.

1-14.7.2 Signature

- 1-14.7.2.1 A In order to fulfil certain card schemes operating regulations, the Terminal shall be able to accept a signature as CVM, if the terminal is attended.
- The PSAM controls the CVM.
- 1-14.7.2.2 A It must be possible for the merchant to force the CVM to be signature provided that the card scheme for the Card in question indicates this as being legal.
- NOTE:** If the Card used is an ICC, the CVR indicates whether or not it is allowed for the merchant to force the CVM to be signature.

1-14.8 Protected Functions

1-14.8.1 General Requirements

Certain terminal functions are critical and should be protected so only authorized users have access to these functions. An example could be the Refund transaction where funds will be moved from the merchant's account to a cardholder's account.

A supervisor mode may also allow more administrative functions, such as Installation and PSAM Deactivation, than the normal operating mode available to all the clerks.

- | | | |
|------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-14.8.1.1 | C | The terminal may have a 'lock' function implemented by which functions can be blocked individually or in groups. Implementation of the 'lock' function is manufacturer specific and may be based on a physical lock, passwords/PINs and/or special cards. |
| 1-14.8.1.2 | C | The 'lock' function may be managed by the merchant and the 'lock' function shall allow the merchant to authorize clerks individually. |
| 1-14.8.1.3 | C | The 'lock' function may be implemented as part of the Merchant Application. |
| 1-14.8.1.4 | B | The Refund transaction shall be protected by a 'lock' function, to ensure that only authorized clerks will be able to initiate Refund transactions |

1-14.8.2 Protected Functions - Manufacturer Specific Functions

Certain terminal functions are very critical and shall be protected so only the Terminal Supplier have the access to these functions (e.g. reset of Data Store).

- | | | |
|------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-14.8.2.1 | A | Critical functions only allowed to be initiated by the Terminal Supplier, shall be protected by a 'Technician lock' function. Implementation of the 'Technician lock' function is manufacturer specific and may be based on a physical lock, password/PIN and/or special cards. |
| 1-14.8.2.2 | A | The 'Technician lock' function shall be managed by the Terminal Supplier and the 'Technician lock' function shall allow only the Terminal Supplier's authorized personnel to initiate the protected functions. |
| 1-14.8.2.3 | A | If the 'key' to the 'Technician lock' is common for terminals installed at several Merchants, only the Terminal Supplier shall be able to produce 'copies' of the 'key'. |
| 1-14.8.2.4 | B | If the 'key' to the 'Technician lock' is based on a password or PIN, the 'key' shall be dynamically assigned (i.e. a new password each day), and it shall not be possible to predict the value of a 'key' based on the knowledge of a previous 'key'. |

1-14.9 Reports

1-14.9.1 General Requirements

- 1-14.9.1.1 A The following reports shall be generated:
- Batch Report
- 1-14.9.1.2 A The Batch Report shall include the necessary data for the merchant to perform an appropriate balancing between the Batch Reports and the settlement statements generated by the acquirer.
- 1-14.9.1.3 C Reports for the following transaction types may be printed:
- Balancing Report (counters, turnover etc., specified by the Terminal Supplier)
 - Installation Report
 - PSAM Deactivation Report
 - PSAM Update Report

1-14.10 Log

1-14.10.1 Requirements

- 1-14.10.1.1 B Entries in the Log shall be retained for a minimum of 18 months.
- 1-14.10.1.2 A All transactions results shall be stored in the Log, irrespective of the result.
- 1-14.10.1.3 A It shall be possible to readily make a plaintext print-out or a copy of the Log.
- 1-14.10.1.4 A Upon request, a print-out of the Log shall either include one transaction or a sequence of transactions.
- 1-14.10.1.5 A In case of electronically stored logs, it shall be possible to, in a period of 24 hours (1 working day), generate a print out of the interval to be evaluated.
- 1-14.10.1.6 A If the log is implemented as a "paper-log", the printing technology and paper used shall assure 100% readability after proper storage of the original receipt according to the current local legislative requirements.
- 1-14.10.1.7 B If the log is stored on an electronic media with limited capacity and the storage area reserved for the log becomes full or nearly full of log messages, the merchant shall be informed and requested to erase/delete the oldest log messages.
- 1-14.10.1.8 B If the log stored on an electronic media with limited storage capacity, the merchant shall have access to service functions by means of which the merchant is able to perform one or more of the following procedures:

- Make a printed copy of the oldest log messages
 - Move the oldest log messages to another media
 - Delete the oldest log messages
- 1-14.10.1.9 B If service functions as described in 1-14.10.1.8 is available, at least one of the following functions shall be supported:
- Make a printed copy of the oldest log messages or
 - Move the oldest log messages to another media.
- 1-14.10.1.10 B If service function for deleting the oldest log message is supported as described in 1-14.10.1.8, the merchant shall be encouraged to delete as few as possible of the messages.
- 1-14.10.1.11 A Access to the log shall be protected in such a way that only authorized persons can see and/or print the log data.

Log and PCI

- 1-14.10.1.12 A Additional cardholder data shall be protected according to ref. 35: "Payment Card Industry Data Security Standard".

NOTE: See section 1-7.1.4 page 1-7-3, Transaction Log

Reference

See section 2-4.9.1 page 2-4-14, Log.

1-14.11 Local PIN

See also chapter 2-12 page 2-12-1, Local PIN.

1-14.11.1 Business Requirements

Local PIN described in this section fulfills the following business requirements:

- When the PIN is sent to the PSAM, the PSAM shall compare the PIN entered on the PED with the one received.
- The PIN may be sent either in plaintext or enciphered to the PSAM.
- The key management for the related encipherment keys shall be defined.
- The use of the Local PIN shall be enabled/disabled under the control of Nets Denmark A/S.
- The Local PIN functionality shall be independent of card technology.

1-14.12 Transaction Requirements when using a PSAM

1-14.12.1 Payment, Voice Authorization and Stop List

- 1-14.12.1.1 B A terminal shall support Voice Authorization.
- 1-14.12.1.2 C A terminal may support a Stop List.
- 1-14.12.1.3 A Voice Authorization result shall have priority to validation against a Stop List.
- 1-14.12.1.4 A An electronic Stop List shall have priority to validation against a manual Stop List.
- 1-14.12.1.5 B If the Merchant Application is configurable based upon a decision that Voice Authorization in general is never feasible, the merchant shall be able to make the decision of the actual configuration.

1-15 Regional Requirements

1-15.1 Introduction

This chapter specifies requirements that are specific to different regions. The information is listed for a region at a time. The areas covered are;

- Regional functional requirements,
- Regional display (and terminal) texts,
- Regional receipt texts,
- Regional Processing Condition Table.

This chapter contains so far, information for the following regions;

- Denmark (functional req., display texts, receipt texts),
- Sweden (functional req., display texts, receipt texts),
- Norway (functional req, display texts, receipt texts),
- Finland (functional req.),
- Poland (display texts),
- Germany (display texts, receipt texts).

Functional requirements

The regional functional requirements consists of a listing of optional functional requirements, mandatory in a specific region, followed by specific functional requirements that are not a part of the generic requirements.

Display and terminal texts

The regional display texts are tables of display texts, where the English and the regional texts are listed side-by-side. This section will as well contain information on any optional texts used on the enclosure and keypad of the terminal.

Receipt texts

The regional receipt texts are defined in tables. The content of the tables is as follows;

- The first column refers to the line numbers displayed in the generic receipt format, like 'IH5'. The number may be followed by a letter if multiple texts are possible. If the same element is used in multiple lines, then both entries will be shown, separated by a '/'.
- The second column holds the logical name of the element. The name is only mentioned first time, if multiple entries exists for a receipt line. An example of this are the lines 'AM2a' and 'AM2b'.
- The third column holds the English (reference) text.
- The fourth column holds the text in the regional language. The column may hold the entry <blank> if the element is not used in the specific language.
- The text specified in column three and four may span two or more lines. New line is indicated by a '\'

Processing Condition Table

The regional Processing Condition Table's are only applicable to some regions. The response to the commands may vary

from region to region. The tables shown, have the same basic format as the generic response to 2-14.5.12 page 2-14-47 Get Processing Table.

1-15.1.1 Generic Requirements

This section handle requirements that are generic with respect to handling of different languages.

- 1-15.1.1.1 A It is required that the terminal is EMV compliant. Ref. 20: "EMV ICC Specification" Book4 section 11 contains requirements for language selection. The requirements in this section shall be fulfilled if the terminals is to be EMV compliant.
- The terminal may be able to support more than one language for the display texts used on the Cardholder Display, as defined in section 2-4.8.1 page 2-4-10, "Sub-handler, Cardholder Display".
- 1-15.1.1.2 C If the terminal supports more than one language for the text on the Cardholder Display, the cardholder may be able to select the actual language manually.
- NOTE:** The language used on the merchant display shall according to "EMV ICC Specification", ref. 20 always be the merchants local language.
- 1-15.1.1.3 C The cardholder may be able to select the actual language both before the transaction is initiated and/or during the transaction flow.
- NOTE:** The selection of language during the transaction flow may be limited due to the actual implementation.
- 1-15.1.1.4 B When a transaction is completed and the terminal returns to idle state (ready to service a new cardholder), the cardholders display shall automatically select the merchants local language as the default language.
- 1-15.1.1.5 B If a cardholder has selected a language but no transaction has been initiated (i.e. no card inserted), the terminal shall after a pre-defined time-out value automatically shift back to the default language, i.e. the merchant local language.
- NOTE:** The Time-out value may depend on the environment in which the terminal is used.
- 1-15.1.1.6 C The display texts shall be taken from the localization definitions found in this section 1-15, "Regional requirements".

1-15.1.2 ICC Language Selection

The ICC may include the data element Language Preference (tag '5F2D').

- | | | |
|------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-15.1.2.1 | A | If the terminal supports more than one language, the terminal shall be able to set the language to be used based on this data element in the ICC. |
| 1-15.1.2.2 | A | The ICC Language Selection shall be performed according to ref. 20: "EMV ICC Specification". |
| 1-15.1.2.3 | A | Language selection based on the data element Language Preference shall be performed before the <i>Initiate EMV Payment</i> command is initiated. |
| 1-15.1.2.4 | B | Language selection based on the data element Language Preference shall overrule any language selection performed manually prior to inserting the ICC. |
| 1-15.1.2.5 | B | If the data element Language Preference is not supported by the ICC, and the terminal supports more than one language, the terminal shall allow the cardholder to select the preferred language, as if the data element Language Preference was supported but no match were found. |
| 1-15.1.2.6 | C | The terminal may allow the cardholder to select the language manually after the selection based on the data element Language Preference has been completed. |

1-15.2 Denmark

1-15.2.1 Danish Regulations

Basic Regulations

All terminal operation within the Danish banking system must comply with certain regulations as set up by Nets Denmark A/S, the Danish Banking Association and Danish legislation. These regulations form the basis for several requirements especially when handling chip and magnetic stripe cards and PINs.

A basic requirement for handling the cards is that the cardholder by default handles his/her card, enters the PIN and accepts the amount by himself/herself.

The terminal allows more acquirers to use the same terminal for different brands of cards. This requires the terminal architecture to be open for more applications and related communication to the acquirers.

The Dankort Handbook

The Danish debit card scheme, Dankort, is regulated in ref. 34: "Dankort-regler", including updates to the document, which sets up requirements, especially for the handling of PINs.

The requirements in the Dankort-regler must be complied with for all terminals handling the Dankort. The requirements in the handbook are reflected in the functional requirements and the design requirements in this specification.

Secure Handling of PINs

It is a firm requirement that PINs must never be present in plaintext outside the physically and logically protected devices, i.e. the PIN entry Device (PED)/PIN Pad, the PSAMs and the host crypto modules.

1-15.2.2 Functional Requirements

Adding Tip/Gratuity

- 1-15.2.2.1 A If tips/gratuity is added to the electronic transaction after the cardholder has accepted the transaction (Method 4), the amount added as gratuity shall not exceed any of the following conditions:
- 15% of (Amount for Goods and Services + any Surcharge)
 - 1000 DKK

- 1-15.2.2.2 A If the actual transaction currency is different from DKK, the absolute limit shall correspond to 1000 DKK.

When the exact amount is known while the card is present in the terminal, and PIN is used as CVM, the cardholder also accepts the amount to pay for goods and service (including any surcharge) during the sequence.

Handling of Dankort

- 1-15.2.2.3 A For the co-branded Visa/Dankort, the terminal shall handle the card as a Dankort in terminals accepting Dankort.

NOTE: The Visa/Dankort has one AID (Visa), only.

NOTE: The Visa/Dankort is recognized by the BIN starting '4571'.

- 1-15.2.2.4 A If the terminal accepts Dankort, the terminal shall be capable of setting the terminal parameters specific for the handling of the Dankort.

No CVM

- 1-15.2.2.5 A Terminals supporting No CVM shall have an an individual acceptance from the acquirers including Nets Denmark A/S.

Payment Condition Code

- 1-15.2.2.6 C A Danish terminal may implement Payment Condition Code as specified in section 1-10.5.6 page 1-10-17.

Business Calls

- 1-15.2.2.7 A Danish Terminals may use the the terms for business calls as specified in table 1-11.2.

1-15.2.3 Issuer Information Envelope Data

- 1-15.2.3.1 C A Danish Terminal may support Issuer Envelope Data for all types of transactions. The data shall be TLV encoded. Tag "Z0" is reserved for private use.

- 1-15.2.3.2 A The terminal shall ensure that *all* Issuer Envelope Data are concatenated, before the call to *Set Debit/Credit Properties*.

- 1-15.2.3.3 A Only data elements related to the current transaction shall be present in the Issuer Envelope.

NOTE: A data element consists of Tag, Length, and Value. A data elements with a length of 0 is thus not legal.

1-15.2.4 Danish Regional Receipts Requirements

This section contains the specific Danish requirements. see section 1-15.2.8 for detailed text requirements.

- 1-15.2.4.1 A The legislation states that the cardholder shall be able to get a receipt when the cardholder has accepted the payment.
- 1-15.2.4.2 A Table 1-15.5 page 1-15-13 defines the regional Danish texts that shall be used when printing receipts.
- 1-15.2.4.3 A A regional Danish receipt shall contain all the mandatory lines from the blocks in the generic receipt.
- 1-15.2.4.4 C A regional Danish receipt may omit the lines HI6, HI7 and HI8 for a purchase transaction for Goods and Services.
- 1-15.2.4.5 A The regional Danish display texts shall be as defined in section 1-11.1 page 1-11-2.
- 1-15.2.4.6 A A regional Danish receipt shall, in the Merchant Information block always have the following lines (not mandatory in the generic receipt);
- MI4 (Phone number) and
 - MI5 (Bus. reg. number).
- 1-15.2.4.7 C The information for lines MI4 and MI5 may be provided in a preprinted part of the receipt.
- 1-15.2.4.8 C A regional Danish receipt should *not* have the line AM3 (VAT) in the Amount Information block.
- 1-15.2.4.9 B A regional Danish receipt shall not have the line TR1 (PIN used) in the Transaction Information block.
- 1-15.2.4.10 C A regional Danish receipt should not have the line TR4 (Account Type Selection) in the Transaction Information block.
- 1-15.2.4.11 A A regional Danish receipt shall, when it is a Purchase with tips using method 4 (see section 1-10.15.5), have the "Tips Informative Message" in Danish, SI2 - SI3, as well as in English, SI4 - SI5.
- 1-15.2.4.12 C A regional Danish receipt may in the lines TR14, field "Transaction result" use the text "GENNEMFØRT" when the following conditions are met;
- the transaction has been completed successfully and
 - all messages with financial impact have been transferred successfully to the host.
- NOTE:** This implies for an OTRS terminal, that a Financial Request (MTI 0206 or 0207) has been exchanged successfully as part of the transaction.
- 1-15.2.4.13 A The <conversion provider> for DCC transactions shall be "Teller A/S".

1-15.2.5 Key Legend

- 1-15.2.5.1 C Terminals installed in Denmark, may use the following national texts on the keypad.

Table 1-15.1 - Command Keys

Key	Danish key legend
"CANCEL"	"SLET ALT"
"CLEAR"	"SLET"
"ENTER"	"GODKEND"

- 1-15.2.5.2 C Terminals installed in Denmark should use the texts specified in table 1-15.2 for the different business calls.

Table 1-15.2 - Business Calls and Service Functions (Danish)

English	Danish (20 characters)	Danish (16 characters)
Purchase	Køb eller Betaling*	Køb
Refund	Retur	Retur
Original/Extended Authorization	Autorisation	Autorisation
Supplementary Authorization	Tillægsautorisation	Tillægsaut.
Reversal (Authorization)	Annuller autorisation	Annuller Aut.
Capture	Capture	Capture
Cancellation	Annullering	Annullering
Top Up	Kontant opladning	Kontant opladn
Gratuity or Extra	Ekstra	Ekstra
Post Purchase	Sent køb	Sent køb
Post Refund	Sen retur	Sen retur

Legend: * = The most suitable name may be selected.

- 1-15.2.5.3 A A terminal installed in Denmark shall use the following texts, listed in table 1-15.3 for the different Administrative Functions.

Table 1-15.3 - Administrative Functions (Danish)

English	Danish
Installation	Installation
Advice Transfer	Afstemning or Aflevering*
Clock Synchronization	Synkroniser Ur
PSAM Update Transfer	Opdater PSAM
PSAM Deactivate	Afmeld PSAM

Legend: * = The most suitable name may be selected.

1-15.2.6 Display Characters

- 1-15.2.6.1 A The Cardholder Display shall in addition to the capital letters: "A" - "Z", be able to show the Danish capital letters: "Æ", "Ø", and "Å".
- 1-15.2.6.2 C The Cardholder Display may in addition to the lower case letters: "a" - "z", be able to show the Danish letters: "æ", "ø", and "å".

1-15.2.7 Display Texts

- 1-15.2.7.1 A Below is table 1-15.4 that defines the regional texts that shall be used when displaying text where Danish is the language chosen.

Table 1-15.4 - Messages for Display (Danish)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'01'	(Amount)	(Beløb)	(Amount)	(Beløb)
'02'	(Amount) OK?	Godkend (Beløb)	(Amount) OK?	Godkend (Beløb)
'03'	Approved	Godkendt	Approved	Godkendt
'04'	Call Your Bank	Kontakt din bank	Call Your Bank	Kontakt din bank
'05'	Cancel or Enter	Slet alt / Godkend	Cancel or Enter	Slet alt / Godkend
'06'	Card Error	Kort fejl	Card Error	Kort fejl
'07'	Declined	Afvist	Declined	Afvist
'08'	Enter Amount	Indtast beløb	Enter Amount	Indtast beløb
'09'	Enter PIN	Tast PIN	Enter PIN	Tast PIN
'0A'	Incorrect PIN	Forkert PIN	Incorrect PIN	Forkert PIN
'0B'	Insert Card	Indlæs kort	Insert Card	Indlæs kort
'0C'	Not Accepted	Kan ikke anvendes	Not Accepted	Kan ej anvendes
'0D'	PIN OK	PIN OK	PIN OK	PIN OK
'0E'	Please Wait	Vent	Please Wait	Vent
'0F'	Processing Error	Teknisk fejl	Processing Error	Teknisk fejl
'10'	Remove Card	Husk kortet	Remove Card	Husk kortet
		Tag kortet		Tag kortet
'11'	Use Chip Reader	Brug chipkortlæser	Use Chip Reader	Brug chipkort
'12'	Use MAG Stripe	Brug magnetkortlæser	Use MAG Stripe	Brug magnetkort
'13'	Try Again	Prøv igen	Try Again	Prøv igen
'14'	Welcome	Velkommen	Welcome	Velkommen
'15'	Present Card	Placer kortet	Present Card	Placer kortet
'16'	Processing	Behandler	Processing	Behandler
'17'	Card read OK. Please remove card	Kortet er læst Tag kortet	Card read OK Remove card	Kortet er læst Tag kortet
'18'	Insert or swipe card	Indlæs kort	Insert/swipe crd	Indlæs kort
'19'	Use one card only	Mere end et kort!	One card only	Kun et kort!

Table 1-11.1 - Messages for Display (Danish) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'1A' – '3F'	RFU for assignment by EMV			
'40'	System Error, retry	Systemfejl prøv igen	System Error	Systemfejl
'41'	Invalid Card	Ugyldigt kort	Invalid Card	Ugyldigt kort
'42'	Card out-of-order	Kortet virker ikke	Error in card	Fejl i kort
'43'	Expired Card	Kort udløbet	Expired Card	Kort udløbet
'44'	Insufficient value	For lav restværdi	Too low value	For lav værdi
'45'	Card not present	Kort ej tilstede	Card missing	Kort ej tilstede
'46'	Data Store full	Datalager fyldt	Data Store full	Datalager fyldt
'47'	Timed out	Time-out!	Timed out	Time-out!
'48'	Thank You	Tak!	Thank You	Tak!
'49'	Not available	Ikke tilgængelig	Not available	Ikke tilgængelig
'4A'	Print receipt?	Ønskes kvittering?	Print receipt?	Kvittering?
'4B'	Cancel	Annullér	Cancel	Annullér
'4C'	Make Selection	Vælg	Make Selection	Vælg
'4D'	Incorrect Amount	Forkert beløb	Wrong Amount	Forkert beløb
'4E'	Welcome	Velkommen	Welcome	Velkommen
'4F'	Signature	Underskrift	Signature	Underskrift
'50'	Application Menu	Menu	Menu	Menu
'51'	Transaction Menu	Menu	Menu	Menu
'52'	Purchase	Køb	Purchase	Køb
'53'	Page	Side	Page	Side
'54'	PIN Blocked	PIN-spærret	PIN Blocked	PIN-spærret
'55'	Enter New PIN	Indtast ny PIN	Enter New PIN	Indtast ny PIN
'56'	PIN Changed	PIN er ændret	PIN Changed	PIN er ændret
'57'	PIN Unchanged	PIN ikke ændret	PIN Unchanged	PIN ikke ændret
'58'	2 PINs not same	2 PIN ikke ens	2 PINs not same	2 PIN ikke ens
'59'	Confirm new PIN	Bekræft ny PIN	Confirm new PIN	Bekræft ny PIN
'5A'	Change PIN	Ændr PIN	Change PIN	Ændr PIN
'5B'	Unblock PIN	Frigiv PIN	Unblock PIN	Frigiv PIN
'5C'	PIN not blocked	PIN ikke spærret	PIN not blocked	PIN ikke spærret
'5D'	PIN Unblocked	PIN frigivet	PIN Unblocked	PIN frigivet
'5E'	Calling...	Opkald...	Calling...	Opkald...
'5F'	Transmitting...	Sender...	Transmitting...	Sender...
'60'	Receiving...	Modtager...	Receiving...	Modtager...
'61'	Comms Error	Kommunikationsfejl	Comms Error	Kommunik. fejl
'62'	Disconnecting	Afbryder	Disconnecting	Afbryder
'63'	Trans Log Upload	Trans.log sendes	Trans Log Upload	Trans.log sendes
'64'	Retrying	Prøver igen	Retrying	Prøver igen
'65'	Upload Done	Afsendelse OK	Upload Done	Afsendelse OK

Table 1-11.1 - Messages for Display (Danish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'66'	Upload Failed	Fejl i afsendelse	Upload Failed	Fejl i afsend.
'67'	No Records	Ingen data	No Records	Ingen data
'68'	Debit:	Debet:	Debit:	Debet:
'69'	Credit:	Kredit:	Credit:	Kredit:
'6A'	Credit Reversal	Kredit tilbageførsel	Credit Reversal	Kredit retur
'6B'	Cash Load	Kontant opladning	Cash Load	Kontant opladn.
'6C'	Balance:	Saldo:	Balance:	Saldo:
'6D'	New Balance	Ny saldo	New Balance	Ny saldo
'6E'	Specify Amount	Angiv beløb	Specify Amount	Angiv beløb
'6F'	Recovery Needed	Fejlretning påkrævet	Recovery Needed	Ret fejl
'70'	Insufficient Funds	Beløb for højt	Value too high	Beløb for højt
'71'	Recovery Failed	Fejlretning ikke OK	Recovery Failed	Fejl ikke rettet
'72'	Recovery Done	Fejlretning OK	Recovery Done	Fejlretning OK
'73'	Money Taken	Beløbet er trukket	Money Taken	Beløbet trukket
'74'	Show Balance	Vis saldo	Show Balance	Vis saldo
'75'	Statement Review	Se kontoudtog	Statement Review	Se kontoudtog
'76'	by issuer	af udsteder	by issuer	af udsteder
'77'	Upload Time	Afsendelsestid	Upload Time	Afsendelsestid
'78'	Start (HH:MM)	Start(tt:mm)	Start (HH:MM)	Start(tt:mm)
'79'	End (HH:MM)	Slut(tt:mm)	End (HH:MM)	Slut(tt:mm)
'7A'	Prefix Nr	Præfix nr.	Prefix Nr	Præfix nr.
'7B'	Totals	Totaler	Totals	Totaler
'7C'	Auth X25 No	Auth. X.25 Nr	Auth X25 No	Auth. X.25 Nr
'7D'	Upload X25 No	Afsendelses X.25 Nr	Upload X25 No	Afsend. X.25 Nr
'7E'	No Trials:	Nr forsøg	No Trials:	Nr forsøg
'7F'	Delay:	Forsinkelse:	Delay:	Forsinkelse:
'80'	Onl Auth. Data	Online auth. data	Onl Auth. Data	Online auth.
'81'	Onl Upload Data	Online batch data	Onl Upload Data	Online batch
'82'	Get Cash	Kontanthævning	Get Cash	Kontanthævning
'83'	Unblock Appli.	Ophæv appl. spærring	Unblock Appli.	Lås appl. op
'84'	Pre-Autho.	Præautorisation	Pre-Autho.	Præautorisation
'85'	Pre Completion	Foreløbig afslutning	Pre Completion	Foreløbig afslut
'86'	Refund:	Retur:	Refund:	Retur:
'87'	Cancellation	Annullering	Cancellation	Annullering
'88'	D/C Menu	D/K menu	D/C Menu	D/K menu
'89'	Precomp. Number	Forudberegn nummer	Precomp. Number	Forudberegn nr.
'8A'	Get Merchant PIN	Forretnings PIN	Get Merchant PIN	Forretnings PIN
'8B'	Data required in the DB	Data krævet i base	Need data in DB	Data krævet

Table 1-11.1 - Messages for Display (Danish) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'8C'	Interval (MM)	Interval (mm)	Interval (MM)	Interval (mm)
'8D'	Number Attempts	Antal forsøg	Number Attempts	Antal forsøg
'8E'	Load Stop List	Load spærreliste	Load Stop List	Load spærreliste
'8F'	Pick up Card	Spærret – inddrag	Pick up Card	Spærret: Inddrag
'90'	Denied:	Afvist:	Denied:	Afvist:
'91'	View Balance?	Se saldo?	View Balance?	Se saldo?
'92'	Do not honor	Afvist	Do not honor	Afvist
'93'	Expired Card	Kort udløbet	Expired Card	Kort udløbet
'94'	Suspected fraud	Mulig svindel	Suspected fraud	Mulig svindel
'95'	PIN exceeded	For mange PIN forsøg	PIN exceeded	PIN-spærret
'96'	Refer Issuer	Kontakt kortudsteder	Refer Issuer	Kontakt udsteder
'97'	No card number	Intet kortnummer	No card number	Intet kortnummer
'98'	Excessive Amount	For højt beløb	Excessive Amount	For højt beløb
'99'	Counterfeit Card	Falsk kort	Counterfeit Card	Falsk kort
'9A'	Format Error	Formatfejl	Format Error	Formatfejl
'9B'	Card issuer or	Kortudsteder eller	Card issuer or	Udsteder eller
'9C'	Switch inop.	Switch ude af drift	Switch inop.	Switch fejl
'9D'	Bad Routing	Forkert rutning	Bad Routing	Forkert rutning
'9E'	Sys malfunction	Systemfejl	Sys malfunction	Systemfejl
'9F'	Yes	Ja	Yes	Ja
'A0'	No	Nej	No	Nej
'A1'	Capture Card	Inddrag kort	Capture Card	Inddrag kort
'A2'	Money not taken	Beløb ej trukket	Money not taken	Beløb ej trukket
'A3'	Exp. date (YYMM)	Udløbsdato (ÅÅMM)	Exp. date (YYMM)	Udløb (ÅÅMM)
'A4'	Enter PAN	Indtast kortnummer	Enter PAN	Indtast kortnr.
'A5'	Enter Term ID	Indtast terminal ID	Enter Term ID	Indtast term. ID
'A6'	Params Required	Parametre krævet	Params Required	Parametre krævet
'A7'	Forced online	Online krævet	Forced online	Online krævet
'A8'	Sale:	Salg:	Sale:	Salg:
'A9'	Refund:	Tilbagebetaling:	Refund:	Tilbagebetaling:
'AA'	Purse empty	Pungen er tom	Purse empty	Pungen er tom
'AB'	Set currency	Angiv valuta	Set currency	Angiv valuta
'AC'	Currency changed	Valutakode ændret	Currency changed	Valuta ændret
'AD'	Terminal ID	Terminal ID	Terminal ID	Terminal ID
'AE'	Exceeds limit	Grænse overskredet	Exceeds limit	Over grænse
'AF'	Invalid currency	Ugyldig valuta	Invalid currency	Ugyldig valuta
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	Terminalen er klar	Terminal ready	Terminal er klar
'E1' 1)	No receipt	Ingen kvittering	No receipt	Ingen kvittering

Table 1-11.1 - Messages for Display (Danish) (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'E2'				
'E3'	Error reading card	Fejl ved kortlæsning	Card read error	Fejl ved læsning
'E4'	Card validated	Kort godkendt	Card validated	Kort godkendt
'E5'	Receipt wanted?	Ønskes kvittering?	Receipt wanted?	Kvittering?
'E6'	Printing receipt	Kvittering udskrives	Printing receipt	Kvitt. udskrives
'E7'	Purchase interrupted	Købet er afbrudt	Purchase stopped	Købet er afbrudt
'E8'	Terminal failure	Fejl i terminalen	Terminal failure	Terminalfejl
'E9'	Terminal busy	Terminal er optaget	Terminal busy	Terminal optaget
'EA'	Out of order	Ude af drift	Out of order	Ude af drift
'EB'	Push	Tryk	Push	Tryk
'EC'	Enter PIN and Accept	Tast PIN og Godkend	Enter PIN/Accept	Tast PIN/Godkend
'ED'	Swipe card	Indlæs kort	Swipe card	Indlæs kort
'EE'	Insert card again	Indlæs kort igen	Insert card	Indlæs kort igen
'EF'	PIN:	PIN:	PIN:	PIN:
'F0'	Buy:	Køb:	Buy:	Køb:
'F1'	Accept?	Tast Godkend	Accept?	Tast Godkend
'F2'	Bonus added	Bonus noteret	Bonus added	Bonus noteret
'F3'	Technical failure	Teknisk fejl	Tech. failure	Teknisk fejl
'F4'	Try again later	Prøv igen om lidt	Try again later	Prøv igen senere
'F5'	Limit reached	Maksimum er udnyttet	Limit reached	Max. er udnyttet
'F6'	Card is blocked	Kortet er spærret	Card is blocked	Kortet spærret
'F7'	Refer Acquirer	Ring indløser	Refer Acquirer	Ring indløser
'F8'	(X) PIN tries left	(X) PIN forsøg igen	(X) PIN tries left	(X) PINforsøg igen
'F9'	Invalid merchant	Ukendt forretning	Invalid merchant	Ukendt forretn.
'FA'	Card unknown	Kortet er ukendt	Card unknown	Kortet er ukendt
'FB'	Split payment?	Delt betaling?	Split payment?	Delt betaling?
'FC'	Card/amount recorded	Kort/beløb noteret	Data recorded	Data noteret
'FD'	Identical purchase	Identisk køb udført	Identical trans.	Identisk køb
'FE'	(Action Code)	(Action Code)	(Action Code)	(Action Code)
'FF'	Invalid transaction	Ugyldig transaktion	Invalid trans.	Ugyldig trans.

Legend: ¹⁾ The message may flash on the display to attract the cardholder's attention.

²⁾ A “-” or a “+” may be used instead of the “/”.

Generally, when “(“and”) are used, the actual value of whatever is inside the brackets is indicated.

(X) indicates actual value.

Message Codes 'EC' and 'F1' are proposed text

1-15.2.8 Receipt Texts

1-15.2.8.1 A Below is table 1-15.5 that defines the regional Danish texts that shall be used when printing receipts.

Table 1-15.5 - Messages for printing (Danish)

Receipt Line	Element	English	Danish
'MI4'	Phone	Phone:	TLF.
'MI5'	Business Reg. number	Buss.Reg.No:	CVR. NR.
'HI2'	Copy indicator	Copy	Kopi
'HI4a'	Prelim/post indicator	Preliminary	Foreløbig
'HI4b'	Prelim/post indicator	Post registration	Efterregistrering
'HI4c'	Cancellation indicator	Cancellation	Annullering
'IH5'	Non-financial indicator	This is not a receipt	Ikke en kvittering
'HI7a'	Transaction indicator	Authorization only	Kun autorisation
'HI7b'		Refund	Retur
'HI7c'		Reversal (auth)	Annullering (Aut)
'HI7d'		Cancellation	Sletning
'HI7e'		Cash	Cash
'AM2a'	Amount type	Purchase	Køb
'AM2b'		Refund	Retur
'AM2c'		Cash	Cash
'AM2d'		Amount	Beløb
'AM4'	V.A.T.	VAT incl.	Heraf moms
'AM5'	Surcharge	Surcharge	Gebyr
'AM6'	Cashback	Cashback	Byttepenge
'AM7' / 'AM11'	Extra	Extra	Ekstra
'AM9' / 'AM13'	Total	Total	Total
'TR1'	PIN indicator	PIN used	Med PIN
'TR3'	Payment code	Paym.code:	Betalingskode
'TR4a'	Account type	Saving transaction	<blank>
'TR4b'		Debit transaction	<blank>
'TR4c'		Credit transaction	<blank>
'TR8'	Merchant number	Me.No:	Nets no:
'TR12'	Status	Status:	Status:
'TR13'	Auth.code	Auth.code:	Aut.kode:
'TR14a'	Auth.result	Authorized	Autoriseret
'TR14b'		Authorized	Gennemført
'SI2/SI4'	Tips info – 1	** When tipping **	** Ved ekstra **
'SI3/SI5'	Tips info – 2	Ask for new receipt	husk ny kvittering
'SI6/SI7'a	Approval message	?Approved for \ crediting of account	<blank>
'SI6/SI7'b		?Approved for debiting\ of account as above	<blank>

Table 1-15.5 - Messages for Printing (Danish) (*concluded*)

Receipt Line	Element	English	Danish
'SI8'	Card reference	Printed digits:	Cifre på kort:
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	Identitetsbevis: \ (Pas e.l.)
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	Udstedt af;
'SI16'	ID expiry date	ID expiry date:	Gyldigt indtil:
'SI18'	Clerk ID	Clerk ID:	Ekspedient:
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholder's account by the issuer	Udsteder kan efterfølgende tilføje et gebyr på transaktionen
'SI26'a	Signatory type	Merchant's signature	Forretningens signatur
'SI26'b		Cardholder's signature	Kortholders signatur
'FI2'a	Termination reason	Interrupted – cancel	Afbrudt – cancel
'FI2'b		Declined	Afvist
'FI2'c		Signature declined	Signatur afvist
'FI2'd		Interrupted – error	Afbrudt – fejl
'FI7'		Keep receipt	Behold notaen
'FI8'a	Recipient indicator	Cardholder's receipt	Kortholders kopi
'FI8'b		Merchant's receipt	Forretningens nota
'PC3'	Balance amount	Balance	Saldo
'PC4'	Expiry date	Exp. date	Udløbsdato
'CL1'	Maximum Deposit	Max Deposit	Max indbetaling
'CL2'	Available Funds	Available Funds	Til opladning
'CL3'	Balance before	Balance before	Kort saldo før
'CL4'	Charge of card	Charge of card	Opladning
'CL5'	Card balance	Card balance	Kort saldo

1-15.3 Sweden

1-15.3.1 Functional Requirements

Cancellation

- 1-15.3.1.1 B Attended terminals intended for installation in Sweden shall support the Cancellation Business call. See section 1-10.2.8.

Tips

- 1-15.3.1.2 B In the Restaurant environment, a Terminal shall support the handling of tips as Cardholder entry of a total amount. The tips shall be handled as "Amount other".

Processing Condition Table

- 1-15.3.1.3 A Terminals intended for installation in Sweden shall support a Processing Condition Table. The data objects listed in table 1-15.6 page 1-15-16 and 1-15.7 page 1-15-16 will be present in the response to the *Get Processing Condition Table* command for a Swedish PCT.
- 1-15.3.1.4 A The terminal shall, in a Swedish environment, be able to process a *successful* response to the *Get Processing Condition Table* command with the format as defined in table 2-14.50 page 2-14-50.
- 1-15.3.1.5 A A terminal implementing a Swedish PCT shall, when receiving a header, decode and process all of the data object defined in table 1-15.6 page 1-15-16. The terminal shall build a decoding table handling all of the elements defined in the data object list, DOL.
- 1-15.3.1.6 A A terminal implementing a Swedish PCT shall, when receiving a body and once the DOL is available, be able to decode all the data elements defined in the DOL.
- 1-15.3.1.7 A The terminal shall decode and store any object defined in table 1-15.6 page 1-15-16, and discards any object **not** defined in table 1-15.6 page 1-15-16.

NOTE: The Swedish DOL below contains all of the applicable objects, i.e. the generic as well as the specific Swedish objects.

Exception Handling

- 1-15.3.1.8 A If the terminal can not retrieve a consistent Processing Condition Table from the PSAM during the initialization sequence, the terminal shall continue the initialization sequence (without the support of a Processing Condition Table).

Table 1-15.6 - List of Primitive Swedish Data Objects in the response to the *Get Processing Condition Table, get header* Command

Primitive Data Objects			
Tag	Attrib.	Length	Comment
'9F1A'	n3	2	Terminal Country Code
'DF60'	b2	2	VERSION _{PCT} . Version of the PCT
'DF61'	b1	1	SUBVERSION _{PCT} . Subversion of the PCT
'DF62'	n6	3	DATE _{PCT} . Date of creation (YYMMDD)
'DF63'	b1	1	Length of each record
'DF64'	b2	2	Total no. of records
'DF65'	n12	6	PCT PAN _{FROM}
'DF66'	n12	6	PCT PAN _{TO}
'DF67'	b1	1	Account Type Selection
'DF68'	b1	1	Cashback
'DF69'	b1	1	Key Enter
'DF6A'	b1	1	BIB (defined but not used)
'DF6B'	b4	4	BIB Amount (defined but not used)
'DF6C'	-	Var.	Data Object list (DOL)
'DF6D'	anp	24	Acquirer Name

NOTE: This is a list of possible objects. The order of the data objects in the header is specified in the command, see table 2-14.50.

Table 1-15.7 - List of Constructed Swedish Data Objects, in the response to the *Get Processing Condition Table, get body* Command

Constructed Data Objects			
Tag	Attrib.	Length	Comment
'E3'	-	var.	Header

NOTE: The order of the data in the body is specified in the DOL in the header.

Terminal services

- 1-15.3.1.9 A A Swedish terminal shall implement Account Type Selection as specified in section 1-10.5.3 page 1-10-15 and enable it based on the PCT or the PDOL.
- 1-15.3.1.10 A A Swedish terminal shall, when Account Type has been selected by the Cardholder, return the information in tag Z6 in the Swedish Additional Transaction Data in the Issuer Information Envelope. See table 1-15.8.
- 1-15.3.1.11 A The terminal shall, for a token transaction, transfer Account Type information from the Authorization to the Capture. This can be done as part of the business specific information in the token.

- 1-15.3.1.12 A The regional Swedish display texts shall be as defined in section 1-15.3.4 page 1-15-26.
- 1-15.3.1.13 A The texts specifying the Account types shall be "Bankkonto" (code = 20) and "Kortkredit" (code = 30).
- 1-15.3.1.14 A A Swedish terminal shall implement handling of VAT, as specified in section 1-10.5.5 page 1-10-16.
- 1-15.3.1.15 A An attended Swedish terminal shall implement Cashback as specified in section 1-10.5.4 page 1-10-16 and enable it based on the PCT.
- 1-15.3.1.16 A An attended Swedish terminal shall implement Key Enter Transactions and enable it based on the PCT.
- 1-15.3.1.17 B A Swedish terminal shall implement Payment Condition Code as specified in section 1-10.5.6 page 1-10-17.
- 1-15.3.1.18 A A Swedish terminal shall implement Acquirer Name printing on the receipt based on the PCT.
- 1-15.3.1.19 A A Swedish terminal shall implement Acquirer Information printing, as specified in 1-10.5.8.

Bank at Partner services

By special agreement between issuers and merchants, the terminal may be used for various bank services, e.g. cash withdrawal, and deposit.

- 1-15.3.1.20 B Implementation of "Bank at Partner" shall be supported.
Specific requirements to the banking services are given below.

General Requirements

- 1-15.3.1.21 A The type of banking service - Processing Code - shall be included in the additional transaction data as shown in table 1-15.8 page 1-15-20.
- 1-15.3.1.22 A All banking services shall always result in an online authorization.
- 1-15.3.1.23 A Banking services shall not be allowed for key entered transactions.

Withdrawal

- 1-15.3.1.24 A A Withdrawal shall be handled as a normal purchase transaction.
- 1-15.3.1.25 A For a Withdrawal transaction, the Processing Code '14' (cash at ME) shall be included in the additional transaction data.

Deposit

- 1-15.3.1.26 A A Deposit shall be handled as a normal refund transaction.
- 1-15.3.1.27 A For a Deposit transaction, the Processing Code '28' (deposit at ME) shall be included in the additional transaction data.

Original deposit

- 1-15.3.1.28 A An Original Deposit shall be handled as a normal refund transaction except for key entered transactions which are not allowed.
- 1-15.3.1.29 A For an Original Deposit transaction, the Processing Code '21' (deposit) shall be included in the additional transaction data.
- 1-15.3.1.30 A If the card issuer supports the balance inquiry transaction, the next two requirements shall be complied to.
If the card issuer does not support the balance inquiry transaction, the transaction is rejected.
- 1-15.3.1.31 C A Balance Inquiry transaction shall be initiated as a normal purchase transaction except for some variable settings in the authorization transaction and for the receipt and log.
NOTE: The exact means to initiate the balance inquiry transaction is TBD.
- 1-15.3.1.32 C The balance received in the authorization request response shall be displayed to the cardholder, only.

1-15.3.2 Swedish Regional Receipt Requirements

- 1-15.3.2.1 A A regional Swedish receipt shall contain all the mandatory lines from the blocks in the generic receipt.
- 1-15.3.2.2 A The regional Swedish receipt texts shall be as defined in section 1-15.3.5 page 1-15-26.
- 1-15.3.2.3 A A regional Swedish receipt shall, in the Merchant Information block always have the following lines (not mandatory in the generic receipt);
- MI4 (Phone number) and
 - MI5 (Bus. reg. number).
- 1-15.3.2.4 C The information for lines MI4 and MI5 may be provided in a preprinted part of the receipt.
- 1-15.3.2.5 C A regional Swedish receipt may omit the lines HI6, HI7 and HI8 for a purchase transaction for Goods and Services.
- 1-15.3.2.6 A A regional Swedish receipt shall, in the Header Information block have the lines HI4 (Cancellation indicator) and HI7 (Transaction type) if it is a cancellation transaction.
- 1-15.3.2.7 A A regional Swedish receipt shall in the Amount Information block have the following lines if the VAT is not already printed on the receipt/ticket (not mandatory in the generic receipt);
- AM3 (VAT)
- 1-15.3.2.8 C A regional Swedish receipt may omit the VAT, if it is an Authorization, as the VAT is not known at this point in time.
- 1-15.3.2.9 A A regional Swedish receipt from the Restaurant environment, shall be able use line AM6 (Cashback).
- 1-15.3.2.10 A A regional Swedish receipt shall have the line TR1 (PIN used) if it is a PIN transaction.

- 1-15.3.2.11 B A regional Swedish receipt shall have the lines TR3 (Payment condition) if this is supported by the card used.
- 1-15.3.2.12 A A regional Swedish receipt shall have line TR4 (Account type) in the Transaction Information block if this is supported by the card used.
- 1-15.3.2.13 A A regional swedish receipt shall have the line TR7 (Acquirer name).
- 1-15.3.2.14 A A regional Swedish receipt shall have the lines SI6 and SI7 (Approval message) in the Signature Information block.
- 1-15.3.2.15 A A regional Swedish receipt shall,if it is a refund transaction, have the lines SI17 and SI18 (Clerk ID) in the Signature Information block on the cardholders receipt. See figure 1-12.8
- 1-15.3.2.16 A A regional Swedish receipt shall,if it is a refund transaction, have the lines SI26 to SI28 (Signatory type) in the Signature Information block on the cardholders receipt.
- 1-15.3.2.17 A A regional Swedish manual cash disbursement receipt shall have the lines SI19 to SI22 (Cash fee info message) on the cardholders receipt. See requirement 1-12.2.10.13.
- 1-15.3.2.18 A A regional Swedish receipt shall, if the transaction was a chip read transaction and did not completed successfully, have a line FI6 (TVR/TSI).
- 1-15.3.2.19 A A regional Swedish receipt shall have the line FI7 (Keep receipt) in the Footer Information block.
- 1-15.3.2.20 A A regional Swedish receipt shall have the line FI8 (Recipient Indicator) in the Footer Information block on the cardholder's receipt. The line FI8 may be absent on the merchant's receipt.
- 1-15.3.2.21 A The <conversion provider> for DCC transactions shall be "Teller A/S".

1-15.3.3 Issuer Information Envelope Data

- 1-15.3.3.1 A A Swedish Terminal shall support Issuer Envelope Data for all types of transactions. The terminal shall be able to forward the data specified in table 1-15.8. The data shall be handled as specified in section 1-10.5.1 page 1-10-11.
- 1-15.3.3.2 A Only data elements related to the current transaction shall be present in the Issuer Envelope. Only non-empty data element shall be transferred.

Table 1-15.8 - Swedish additional transaction data in Issuer Information Envelope

Field	Contents	Format	Size (bytes)	Actual Value
TAG _{SE}	Type of Additional Information, Tag "TZ"	a2	2	'545A'
LEN _{SE}	Length of following value fields	b2	2	var.
TAG _{SEACTYPE}	Type of Additional Information, Tag "Z6"	a2	2	'5A36'
LEN _{SEACTYPE}	Length of following value fields	b2	2	'0001'
Account Type	Ref.:2-15.2.1 , Account Type	n2	1	
TAG _{SEPCON}	Type of Additional Information, Tag "Z7"	a2	2	'5A37'
LEN _{PCON}	Length of following value fields	b2	2	'0006'
Payment Conditions	Ref.: 2-15.2.101, Payment Conditions	an6	6	
TAG _{SEPCODE}	Type of Additional Information, Tag "Z8"	a2	2	'5A38'
LEN _{SEPCODE}		b2	2	'0001'
SE Processing Code	Ref.: 2-15.2.23, Processing Code	n2	1	
TAG _{VAT}	Type of Additional Information, Tag "ZA"	a2	2	'5A41'
LEN _{VAT}	Length of following value fields	b2	2	'0005'
VAT Amount	Ref.: 2-15.2.171, VAT Amount	n10	5	
TAG _{BONUS}	Type of Bonus information, Tag "Z2"	a2	2	'5A32'
LEN _{BONUS}	Length of following value fields	b2	2	'000F'
Bonus data		an15	15	
TAG _{MERCHANTINFO}	Type of Merchant information, Tag "Z3"	a2	2	'5A33'
LEN _{MERCHANTINFO}	Length of following value fields	b2	2	'000F'
Merchant data	E.g. ticket information	an15	15	
TAG _{MISC}	Type of Miscellaneous information, Tag "Z4"	a2	2	'5A34'
LEN _{MISC}	Length of following value fields	b2	2	'0011'
Function Code		an2	2	
Miscellaneous data		an15	15	

NOTE: The use of sub-tags Z8, Z2, Z3 and Z4 is deprecated. The sub-tags have never been used. The sub-tags shall not be used anymore.

1-15.3.4 Display Texts

- 1-15.3.4.1 A Below is table 1-15.9 that defines the regional texts that shall be used when displaying text where Swedish is the language chosen.

Table 1-15.9 - Messages for Display (Swedish)

Message Code	20 Characters Display		16 Characters Display	
	English	Swedish	English	Swedish
'01'	(Amount)	SEK (Belopp)	(Amount)	SEK (Belopp)
'02'	(Amount) OK?	Godkänn (belopp)	(Amount) OK?	Godkänn (belopp)
'03'	Approved	Köp godkänt	Approved	Köp godkänt
'04'	Call Your Bank	Kontakta din bank	Call Your Bank	Kontakta bank
'05'	Cancel or Enter	Avbryt med STOP/ Godkänn	Cancel or Enter	Avbryt med STOP/ Godkänn
'06'	Card Error	Kortfel	Card Error	Kortfel
'07'	Declined	Medges ej	Declined	Medges ej
'08'	Enter Amount	Ange belopp	Enter Amount	Ange belopp
'09'	Enter PIN	Ange din kod	Enter PIN	Ange din kod
'0A'	Incorrect PIN	Fel kod	Incorrect PIN	Fel kod
'0B'	Insert Card	Sätt i kort	Insert Card	Sätt i kort
'0C'	Not Accepted	Godkänns inte	Not Accepted	Godkänns inte
'0D'	PIN OK	Kod OK	PIN OK	Kod OK
'0E'	Please Wait	Vänligen vänta	Please Wait	Vänligen vänta
'0F'	Processing Error	Tekniskt fel	Processing Error	Tekniskt fel
'10'	Remove Card	Ta kortet	Remove Card	Ta kortet
'11'	Use Chip Reader	Använd chipläsare	Use Chip Reader	Använd chipläsare
'12'	Use MAG Stripe	Använd magnetläsare	Use MAG Stripe	Använd mag.läsare
'13'	Try Again	Försök igen	Try Again	Försök igen
'14'	Welcome	Välkommen	Welcome	Välkommen
'15'	Present Card		Present Card	
'16'	Processing		Processing	
'17'	Card read OK. Please remove card		Card read OK. Remove card	
'18'	Insert or swipe card		Insert/swipe crd	
'19'	Please present one card only		Please present one card only	

Table 1-15.9 - Messages for Display (Swedish) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Swedish	English	Swedish
'1A' – '3F'	RFU for assignment by EMV			
'40'	System Error, retry	Systemfel, försök igen	System Error	Systemfel
'41'	Invalid Card	Ogiltigt kort	Invalid Card	Ogiltigt kort
'42'	Card out-of-order	Kortet fungerar inte	Error in card	Kortet fungerar ej
'43'	Expired Card	Kortet har utgått	Expired Card	Kortet utgått
'44'	Insufficient value	För lågt värde kvar	Too low value	För lågt värde kvar
'45'	Card not present	Kort saknas	Card missing	Kort saknas
'46'	Data Store full	Datalager fullt	Data Store full	Datalager fullt
'47'	Timed out	Time-out!	Timed out	Time-out!
'48'	Thank You	Tack!	Thank You	Tack!
'49'	Not available	Inte tillgängligt	Not available	Ej tillgängligt
'4A'	Print receipt?	Önskas kvitto?	Print receipt?	Önskas kvitto?
'4B'	Cancel	Avbryt	Cancel	Avbryt
'4C'	Make Selection	Välj	Make Selection	Välj
'4D'	Incorrect Amount	Fel belopp	Wrong Amount	Fel belopp
'4E'	Welcome	Välkommen	Welcome	Välkommen
'4F'	Signature	Underskrift	Signature	Underskrift
'50'	Application Menu	Meny	Menu	Meny
'51'	Transaction Menu	Meny	Menu	Meny
'52'	Purchase	Köp	Purchase	Köp
'53'	Page	Sida	Page	Sida
'54'	PIN Blocked	Kod spärrad	PIN Blocked	Kod spärrad
'55'	Enter New PIN	Ange ny kod	Enter New PIN	Ange ny kod
'56'	PIN Changed	Kod har ändrats	PIN Changed	Kod har ändrats
'57'	PIN Unchanged	Kod är oförändrad	PIN Unchanged	Kod oförändrad
'58'	2 PINs not same	2 kod inte densamma	2 PINs not same	2 kod inte samma
'59'	Confirm new PIN	Bekräfta ny kod	Confirm new PIN	Bekräfta ny kod
'5A'	Change PIN	Byt kod	Change PIN	Byt kod
'5B'	Unblock PIN	Lås upp kod	Unblock PIN	Lås upp kod
'5C'	PIN not blocked	Kod inte spärrad	PIN not blocked	Kod inte spärrad
'5D'	PIN Unblocked	Kod upplåst	PIN Unblocked	Kod upplåst
'5E'	Calling...	Ringer upp ...	Calling...	Ringer upp ...
'5F'	Transmitting...	Skickar ...	Transmitting...	Skickar ...
'60'	Receiving...	Tar emot ...	Receiving...	Tar emot ...
'61'	Comms Error	Kommunikationsfel	Comms Error	Kommunik. fel
'62'	Disconnecting	Avbryter	Disconnecting	Avbryter
'63'	Trans Log Upload	Trans.logg skickas	Trans Log Upload	Tr.logg skickas
'64'	Retrying	Försöker igen	Retrying	Försöker igen
'65'	Upload Done	Överföring OK	Upload Done	Överföring OK

Table 1-15.9 - Messages for Display (Swedish) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Swedish	English	Swedish
'66'	Upload Failed	Fel i överföring	Upload Failed	Fel i överföring
'67'	No Records	Inga data	No Records	Inga data
'68'	Debit:	Debet:	Debit:	Debet:
'69'	Credit:	Kredit:	Credit:	Kredit:
'6A'	Credit Reversal	Återföring av kredit	Credit Reversal	Återf. av kredit
'6B'	Cash Load	Kontantöverföring	Cash Load	Kontantöverför.
'6C'	Balance:	Saldo:	Balance:	Saldo:
'6D'	New Balance	Nytt saldo:	New Balance	Nytt saldo
'6E'	Specify Amount	Ange belopp:	Specify Amount	Ange belopp:
'6F'	Recovery Needed	Felsökning krävs	Recovery Needed	Felsökning krävs
'70'	Insufficient Funds	För högt belopp	Value too high	För högt belopp
'71'	Recovery Failed	Felsökn. misslyckas	Recovery Failed	Felsökn. misslyckas
'72'	Recovery Done	Felsökning OK	Recovery Done	Felsökning OK
'73'	Money Taken	Beloppet har dragits	Money Taken	Beloppet dragits
'74'	Show Balance	Visa saldo	Show Balance	Visa saldo
'75'	Statement Review	Se kontoutdrag	Statement Review	Se kontoutdrag
'76'	by issuer	av utställare	by issuer	av utställare
'77'	Upload Time	Överföringstid	Upload Time	Överföringstid
'78'	Start (HH:MM)	Start(tt:mm)	Start (HH:MM)	Start(tt:mm)
'79'	End (HH:MM)	Slut (tt:mm)	End (HH:MM)	Slut(tt:mm)
'7A'	Prefix No	Prefixnr	Prefix No	Prefixnr
'7B'	Totals	Totaler	Totals	Totaler
'7C'	Auth X25 No	Att. X.25 nr	Auth X25 No	Att. X.25 nr
'7D'	Upload X25 No	Överföring X.25 nr	Upload X25 No	Överför. X.25 nr
'7E'	No Trials:	Antal försök	No Trials:	Antal försök
'7F'	Delay:	Fördröjning:	Delay:	Fördröjning:
'80'	Onl Auth. Data	Online att. av data	Onl Auth. Data	Online att. data
'81'	Onl Upload Data	Online överf. data	Onl Upload Data	Onl. överf. data
'82'	Get Cash	Kontanthämtning	Get Cash	Kontanthämtning
'83'	Unblock Appli.	Upphäv appl.spärr	Unblock Appli.	Upphäv appl.spärr
'84'	Pre-Autho.	Förattest	Pre-Autho.	Förattest
'85'	Pre Completion	Prel. avslutning	Pre Completion	Prel. avslutning
'86'	Refund:	Retur:	Refund:	Retur:
'87'	Cancellation	Makulering	Cancellation	Makulering
'88'	D/C Menu	D/K-meny	D/C Menu	D/K meny
'89'	Precomp. Number	Förberäkna nummer	Precomp. Number	Förberäkna nr
'8A'	Get Merchant PIN	Handlarens kod	Get Merchant PIN	Handlarens kod
'8B'	Data required in DB	Data krävs i databas	Need data in DB	Data krävs i DB
'8C'	Interval (MM)	Intervall (mm)	Interval (MM)	Intervall (mm)

Table 1-15.9 - Messages for Display (Swedish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Swedish	English	Swedish
'8D'	Number Attempts	Antal försök	Number Attempts	Antal försök
'8E'	Load Stop List	Ladda spärrlista	Load Stop List	Ladda spärrlista
'8F'	Pick up Card	Spärrat – ta kortet	Pick up Card	Spärrat –ta kort
'90'	Denied:	Avvisat:	Denied:	Avvisat:
'91'	View Balance?	Se saldo?	View Balance?	Se saldo?
'92'	Do not honor	Avvisat	Do not honor	Avvisat
'93'	Expired Card	Utgånget kort	Expired Card	Utgånget kort
'94'	Suspected fraud	Eventuellt bedrägeri	Suspected fraud	Event. bedrägeri
'95'	PIN exceeded	För många kod-försök	PIN exceeded	För många försök
'96'	Refer Issuer	Kontakta utställaren	Refer Issuer	Kont. utställaren
'97'	No card number	Inget kortnummer	No card number	Inget kortnummer
'98'	Excessive Amount	För högt belopp	Excessive Amount	För högt belopp
'99'	Counterfeit Card	Falskt kort	Counterfeit Card	Falskt kort
'9A'	Format Error	Formatfel	Format Error	Formatfel
'9B'	Card issuer or	Kortutställare eller	Card issuer or	Kortutställare /
'9C'	Switch inop.	switch ur funktion	Switch inop.	Switch ur funkt.
'9D'	Bad Routing	Fel routing	Bad Routing	Fel routing
'9E'	Sys malfunction	Systemfel	Sys malfunction	Systemfel
'9F'	Yes	Ja	Yes	Ja
'A0'	No	Nej	No	Nej
'A1'	Capture Card	Ta kortet	Capture Card	Ta kortet
'A2'	Money not taken	Belopp ej dragits	Money not taken	Bel. ej dragits
'A3'	Exp. date (YYMM)	Utgångsdatum (ÅÅMM)	Exp. date (YYMM)	Utg.datum(ÅÅMM)
'A4'	Enter PAN	Ange kortnummer	Enter PAN	Ange kortnr.
'A5'	Enter Term ID	Ange terminal-ID	Enter Term ID	Ange term. ID
'A6'	Params Required	Parametrar krävs	Params Required	Parametrar krävs
'A7'	Forced online	Online krävs	Forced online	Online krävs
'A8'	Sale:	Försäljning:	Sale:	Försäljning:
'A9'	Refund:	Återbetalning:	Refund:	Återbetalning:
'AA'	Purse empty	Plånboken är tom	Purse empty	Plånboken är tom
'AB'	Set currency	Ange valuta	Set currency	Ange valuta
'AC'	Currency changed	Valutakod ändrad	Currency changed	Valutakod ändrad
'AD'	Terminal ID	Terminal ID	Terminal ID	Terminal ID
'AE'	Exceeds limit	Gränsen överskridits	Exceeds limit	Över gränsen
'AF'	Invalid currency	Ogiltig valuta	Invalid currency	Ogiltig valuta

Table 1-15.9 - Messages for Display (Swedish) (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	Swedish	English	Swedish
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	Terminalen är klar	Terminal ready	Terminal är klar
'E1' ¹⁾	No receipt	Inget kvitto	No receipt	Inget kvitto
'E2'				
'E3'	Error reading card	Fel vid kortläsning	Card read error	Fel kortläsning
'E4'	Card validated	Kort godkänt	Card validated	Kort godkänt
'E5'	Receipt wanted?	Önskas kvitto?	Receipt wanted?	Önskas kvitto?
'E6'	Printing receipt	Kvitto skrivs ut	Printing receipt	Kvitto skrivs ut
'E7'	Purchase interrupted	Köpet avbryts	Purchase stopped	Köpet avbryts
'E8'	Terminal failure	Fel i terminalen	Terminal failure	Fel i terminalen
'E9'	Terminal busy	Terminalen upptagen	Terminal busy	Term. upptagen
'EA'	Out of order	Ur funktion	Out of order	Ur funktion
'EB'	Push	Tryck	Push	Tryck
'EC'	Enter PIN and Accept	Ange kod och godkänn	Enter PIN/Accept	Ange kod/godkänn
'ED'	Swipe card	Dra kort	Swipe card	Dra kort
'EE'	Insert card again	Sätt i kort igen	Insert card	Sätt i kort igen
'EF'	PIN:	Kod:	PIN:	Kod:
'F0'	Buy:	Köp:	Buy:	Köp:
'F1'	Accept?	Godkänn	Accept?	Godkänn
'F2'	Bonus added	Bonus noterad	Bonus added	Bonus noterad
'F3'	Technical failure	Tekniskt fel	Tech. failure	Tekniskt fel
'F4'	Try again later	Försök igen senare	Try again later	Försök senare
'F5'	Limit reached	Maxgränsen har nåtts	Limit reached	Max. har nåtts
'F6'	Card is blocked	Kortet är spärrat	Card is blocked	Kortet spärrat
'F7'	Refer Acquirer	Ring inlösare	Refer Acquirer	Ring inlösare
'F8'	(X) PIN tries left	(X) Kod-försök kvar	(X) PIN tries left	(X) försök kvar
'F9'	Invalid merchant	Okänd handlare	Invalid merchant	Okänd handlare
'FA'	Card unknown	Kortet är okänt	Card unknown	Kortet är okänt
'FB'	Split payment?	Dela upp betalning?	Split payment?	Dela betalning?
'FC'	Card/amount recorded	Kort/belopp noterat	Data recorded	Kort/bel. noterat
'FD'	Identical purchase	Identiskt köp utfört	Identical trans.	Iden.tiskt köp utfört
'FE'	(Action Code)	(Åtgärds kod)	(Action Code)	(Action Code)
'FF'	Invalid transaction	Ogiltig transaktion	Invalid trans.	Ogiltig trans.

Legend: ¹⁾ The message may flash on the display to attract the cardholder's attention.
²⁾ A “-” or a “+” may be used instead of the “/”.
Generally, when “(“and”) are used, the actual value of whatever is inside the brackets is indicated.
(X) indicates actual value.
Message Codes 'EC' and 'F1' are proposed text

1-15.3.5 Receipt Texts

1-15.3.5.1 A Below is table 1-15.10 that defines the regional Swedish texts that shall be used when printing receipts.

Table 1-15.10 - Messages for Printing (Swedish)

Receipt Line	Element	English	Swedish
'MI4'	Phone	Phone:	<blank>
'MI5'	Business Reg. number	Buss.Reg.No:	Org.No.
'HI2'	Copy indicator	Copy	Kopia
'HI4a'	Prelim/post indicator	Preliminary	Preliminär
'HI4b'	Prelim/post indicator	Post registration	Efterregistrering
'HI4c'	Cancellation indicator	Cancellation	Makulerat
'HI5'	Non-financial indicator	This is not a receipt	Endast information
'HI7a'	Transaction indicator	Authorization only	Endast auktorisation
'HI7b'		Refund	Retur
'HI7c'		Reversal (auth)	Reversering av aukt.
'HI7d'		Cancellation	Makulerat
'HI7e'		Cash	Cash
'AM2a'	Amount type	Purchase	Köp
'AM2b'		Refund	Retur
'AM2c'		Cash	Valuta
'AM2d'		Amount	Belopp
'AM4'	V.A.T.	VAT incl.	Varav moms
'AM5'	Surcharge	Surcharge	Extraavgifter
'AM6'	Cashback	Cashback	Kontant
'AM7' / 'AM11'	Extra	Extra	Extra
'AM9' / 'AM13'	Total	Total	Totalt
'TR1'	PIN indicator	PIN used	Personlig kod
'TR3'	Payment code	Paym.code:	Betalkod
'TR4a'	Account type	Saving transaction	Krediterat konto
'TR4b'		Debit transaction	Belastat bankkonto
'TR4c'		Credit transaction	Belastat kortkredit
'TR8'	Merchant number	Me.No:	Butiksnr.
'TR12'	Status	Status:	Status:
'TR12'	Auth.code	Auth.code:	Aukt.kod:
'TR14'	Auth.result	Authorized	Auktoriserat
'SI2/SI4'	Tips info – 1	** When tipping **	** Vid dricks **
'SI3/SI5'	Tips info –2	Ask for new receipt	Kom ihåg nytt kvitto
'SI6/SI7'a	Approval message	Approved for \ crediting of account	Godkännes f. kreditering\ av mitt konto enl. ovan
'SI6/SI7'b		Approved for debiting\ of account as above	Godkännes f. debitering\ av mitt konto enl. ovan

Table 1-15.10 - Messages for Printing (Swedish) (*concluded*)

Receipt Line	Element	English	Swedish
'SI8'	Card reference	Printed digits:	Kortref:
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	Leg:
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	Utfärdande myndighet
'SI16'	ID expiry date	ID expiry date:	Utgångsdatum leg:
'SI18'	Clerk ID	Clerk ID:	Kassör:
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholders account by the issuer	<blank>
'SI26'a	Signatory type	Merchant's signature	Kassörens signatur
'SI26'b		Cardholders signature	Kundens signatur
'FI2'a	Termination reason	Interrupted – cancel	Annullering
'FI2'b		Declined	Medges ej
'FI2'c		Signature declined	Signatur – Medges ej
'FI2'd		Interrupted – error	Avbruten – Teknisk fel
'FI7'		Retain receipt	Spara kvittot
'FI8'a	Recipient indicator	Cardholders' receipt	Kundens ex.
'FI8'b		Merchant's receipt	<blank>
'PC3'	Balance amount	Balance	Saldo
'PC4'	Expiry date	Exp.date	Utgångsdatum

1-15.4 Norway

1-15.4.1 Functional Requirements

General

- 1-15.4.1.1 A The Terminal shall handle the use of Cashback. It shall be possible to enable and disable the functionality.

Reading a MSC

- 1-15.4.1.2 A The terminal shall when reading a magnetic stripe read track2. The terminal may as well read track 3.

- 1-15.4.1.3 A The terminal shall, if reading track 3, be able to let track 3 data take priority over track 2 when both are present on the card.

NOTE: The only type of cards in Norway using track 3 is Bank Asept, BAX.

- 1-15.4.1.4 A The terminal shall when using track 3 information for MSC selection table use, use a "pseudo-PAN" that consists of position 2 - 5 from the card data concatenated with position 9 - 19 of the card data.

NOTE: Position 2 in the magnetic stripe track 3 contains the first digit following the start sentinel.

Reading an ICC

- 1-15.4.1.5 A The terminal shall, if an BankAsept application is mutually supported, by default select this application, even if there are other applications on the card.

- 1-15.4.1.6 C The terminal may have the capability to select another application on the card.

Time-out waiting for host response

- 1-15.4.1.7 A The usual time-out value of 30 seconds for waiting, when the connection has not been declined by lower layers, (see requirement 2-5.14.4.11) shall be replaced with a time-out value of 40 seconds.

Handling of reversals

- 1-15.4.1.8 A The terminal shall when a Reversal Advice is generated, immediately send it to the host.

NOTE: This is the case when a Cancellation is performed.

Handling of Balance for Automated Fuel Dispensers

- 1-15.4.1.9 B The terminal shall, if the Authorization Request Response is successful, retrieve the balance available. The balance shall be retrieved in the response to *Get Debit/Credit Properties* with an index of '000E', see section 2-14.5.8. The terminal shall ensure that the transaction is limited to the amount available also when the amount is 0,00. The Terminal shall, if a soft error and no balance is returned, use the amount from the Authorization Request as the balance / amount available.

Handling BankAxept Exception Rules

The transaction flow for a BankAxept Exception Rule transaction is depicted in figure 1-15.1.

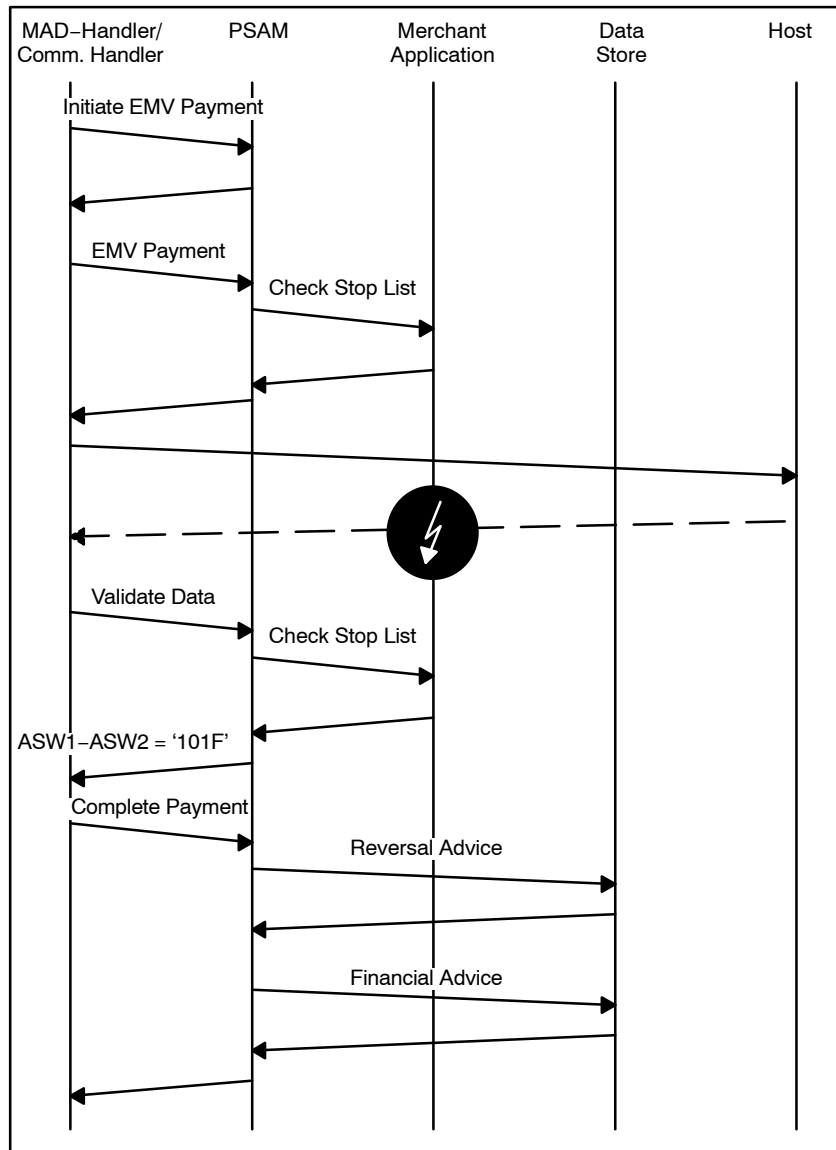


Figure 1-15.1 - BankAxept Exception Rule flow

Note the following characteristics for the BankAxept Exception Rule flow:

- A 2nd *Check Stop List* command is issued by the PSAM during the *Validate Data* phase.
- The PSAM indicates in the response to the *Validate Data* command that the BankAxept Exception Rule is performed by returning an ASW1-ASW2 = '101F' (Exception Rule is successful)
- During the *Complete Payment* phase, two advices will be forwarded to the Data Store. A Reversal of the online request and the resulting Financial Advice.

1-15.4.1.10 A An attended terminal shall implement BankAxept Exception Rule handling.

- 1-15.4.1.11 A The scheme does not allow Cashback for BankAxept Exception Rule. A Bank Axept transaction starting as online cashback shall thus be declined if the online connection is down.
- 1-15.4.1.12 C An attended terminal may implement Cancellation for Bank Axept Exception Rule handling.
- 1-15.4.1.13 A The terminal shall, if BankAxept Exception Rule is enabled accept that the PSAM will generate a second *Check Stop List* command. This command will be issued during the *Validate Data* phase, i.e. after a failed online connection.
- NOTE:** The Terminal will, for a BankAxept Exception Rule Transaction, also receive a *Check Stop List* command during *Payment* phase. This command shall be handled as for normal online transactions.
- 1-15.4.1.14 A The terminal shall when it receives the second *Check Stop List* command prompt the Merchant for acceptance of BankAxept Exception Rule. The terminal shall as well prompt the Merchant for entering an Authorization code. These two actions may be combined.
- 1-15.4.1.15 A The terminal shall return a Stop List Status of;
- '00' if BankAxept Exception Rule is accepted,
 - '80' if BankAxept Exception Rule is declined.
- 1-15.4.1.16 A The terminal shall, if the amount is above 1.500,- NOK ensure that the merchant is prompted for an Authorization Code and that the Authorization Code entered is a 6 digit numeric value.
- 1-15.4.1.17 C The terminal may, if the amount is less than 1.500,- NOK return an "empty" Authorization Code of 6 spaces '20'.
- 1-15.4.1.18 A The terminal shall ensure that the transaction is declined if the ASW returned from the PSAM indicates this.

Norwegian regional receipt requirement

- 1-15.4.1.19 A A regional Norwegian receipt shall contain all the mandatory lines from the blocks in the generic receipt.
- 1-15.4.1.20 A The regional Norwegian texts shall be as defined in section 1-15.4.2 and 1-15.4.3.
- 1-15.4.1.21 A The <conversion provider> for DCC transactions shall be "Teller A/S".
- 1-15.4.1.22 A A regional Norwegian receipt shall, for online transactions print "Acquirer Information" in line TR7 on the receipt. The information shall be retrieved by performing a *Get D/C Properties* command, with an index of '000D' after the *Validate Data* command. See section 2-14.5.8 for more information.
- 1-15.4.1.23 A The terminal shall, for a token transaction, transfer "Acquirer Information" from the Authorization to the Capture. This can be done as part of the business specific information in the token.
- 1-15.4.1.24 C The "Acquirer Information" may cover 2 lines on the receipt, if the information exceeds 24 characters.

- 1-15.4.1.25 C The terminal may, if the transaction is an offline transaction, the terminal has a PCT, and the PCT contains an Acquirer Name, print the name information information in line TR7.
- 1-15.4.1.26 A A regional Norwegian receipt shall, for offline transactions, provide fields for
- space for writing source of and number on Cardholders ID document, lines SI9 - SI12,
 - space for the merchants signature, lines SI16 -SI17.
 - space for the cardholders signature, lines SI26 - SI28.
- 1-15.4.1.27 A A regional Norwegian receipt shall, if the transaction was a chip read transaction and did not complete successfully, have a line FI6 (TVR/TSI).
- 1-15.4.1.28 A A Norwegian receipt shall, if the transaction is performed with a track3 based card (BankAxept) retrieve the PAN to print in line TR5 as the 11 first digits of the PAN returned in the response to the *Init MSC Payment* command.
- 1-15.4.1.29 A A Norwegian receipt shall, if the transaction is performed with a track 3 based card (BankAxept), print the Pan Sequence Number, PSN, on the receipt in line TR2. The PSN shall be retrieved as the last digit of the PAN returned in the response to the *Init MSC Payment* command.
- 1-15.4.1.30 A The terminal shall, for a BankAxept Exception Rule Transaction, generate a set of Norwegian Signature Transaction receipts for an approved transaction.
- 1-15.4.1.31 C The terminal may, for a BankAxept Exception Rule Transaction, if the transaction is declined return a declined PIN or declined Signature receipt.
- 1-15.4.1.32 A A Norwegian receipt shall, if the transaction is a BankAxept Exception Rule transaction, have the line SI6 and SI7 (Approval message) in the Signature Information block.

Norwegian reconciliation

There is, in the regional Norwegian market, a need for a consolidated reconciliation for all of the terminals at a merchants site.

NOTE: A merchant is defined as an entity with a specific business registration number (See field MI5 on the receipt)

NOTE: It is recommended to ensure limited access to the consolidated reconciliation to avoid redundant activation. This could be achieved by letting a supervisor function in the Cash Register system control the activation.

- 1-15.4.1.33 B An attended terminal shall have an operator function to request the generation and reporting of a consolidated reconciliation.
- NOTE:** The value of Message Reason Code in the APACS message shall contain the value '8600' to indicate Reconciliation and subsequent reset of totals.

- 1-15.4.1.34 C The function may be divided into two commands, perform reconciliation and request report.
- 1-15.4.1.35 C An attended terminal may have an operator function to request the generation and reporting of a consolidated turnover since last reconciliation.
- NOTE:** The value of Message Reason Code in the APACS message shall contain the value '8601' to indicate Turnover without reset of totals.
- 1-15.4.1.36 C An unattended terminal may have an automated feature to request the generation and reporting of a consolidated reconciliation.
- 1-15.4.1.37 C The terminal should introduce a delay between the two host requests to allow the host time to process the data.

Generate Consolidated Reconciliation/Turnover

- 1-15.4.1.38 A The message for generating the reconciliation shall be a Network Management Request formatted as specified in table 2-13.71. The Message Reason code shall be as specified in table 2-13.97. The format of the request response will be as shown in table 2-13.72. The Action Code, field 39 in the response shows the status of the request.
- NOTE:** Reconciliation Indicator, field 29 in the response can be used as a reference, when the report is retrieved.
- 1-15.4.1.39 C The terminal may, if the Action Code in the response is '0008', interpret this as an acceptance of the request.
- NOTE:** Reconciliation Indicator, field 29 in the response is the reference value for the report being computed.
- 1-15.4.1.40 C The terminal may, if the Action Code in the response is '5406', generate a new request after a delay.
- NOTE:** Reconciliation Indicator, field 29 in the response is the reference value for the report being computed.
- 1-15.4.1.41 A The terminal shall, if the Action Code in the response is '6013', not generate a new request, before it has retrieved the pending report.
- NOTE:** Reconciliation Indicator, field 29 in the response is the reference value for the report waiting to be retrieved.

Reconciliation/Turnover Report

- 1-15.4.1.42 A The message for requesting a Reconciliation/Turnover Report shall be a Network Management Request formatted as specified in table 2-13.73.
- NOTE:** The format and flow of commands, is similar to the flow when performing PSAM updates.
- 1-15.4.1.43 A The terminal shall use the Reconciliation Indicator, field 29, from the Reconciliation Request Response when requesting the (most recent) report. The format of the the report request response will be as shown in table 2-13.74. The Action Code in the response shows the status of the request.

- 1-15.4.1.44 C The terminal may be able to request previous Consolidated Reconciliation Reports, using previous values of the Reconciliation Indicator, provided that they still are available at the Host.
- 1-15.4.1.45 A The terminal shall, if the Action Code in the response to the Report Request is '5406', generate a new report request after a timeout.
- 1-15.4.1.46 A The terminal shall, if the Action Code in the response to the Report Request is '5412', generate a new reconciliation request after a timeout.
- 1-15.4.1.47 A The terminal shall, if the Action Code in the response to the Report Request is '6022', indicate that the requested report is not available.
- 1-15.4.1.48 A The terminal shall, when the report is available, send a Network Management Notification formatted as specified in table 2-13.75. The terminal shall then receive File Action Instructions as specified in table 2-13.42 and acknowledge as specified in table 2-13.44.
- 1-15.4.1.49 A The terminal shall, when the file transfer is over, wait for a Network Management Notification from the Host, formatted as specified in table 2-13.75.
- 1-15.4.1.50 A The data received in field 63 in the File Action Instructions will be formatted as specified in 2-13.9.19 and shall be concatenated into a Consolidated turnover/reconciliation report, line by line.
- 1-15.4.1.51 A An attended terminal shall be able to request the generation of a consolidated reconciliation.
- 1-15.4.1.52 C An attended terminal may be able to request the result of a consolidated reconciliation.
- 1-15.4.1.53 C An attended terminal may be able to receive and print the result of a consolidated reconciliation.

NOTE: The terminal may have to perform multiple requests, to get all of the information. The response will indicate when all of the information has been retrieved.

1-15.4.2 Display Texts

- 1-15.4.2.1 A Below is table 1-15.11 that defines the regional texts that shall be used when displaying text where Norwegian is the language chosen.

NOTE: A number of additional requirements are defined for the handling of the domestic BankAxept card (BAX).

Table 1-15.11 - Messages for Display (Norwegian)

Message Code	20 Characters Display		16 Characters Display	
	English	Norwegian	English	Norwegian
'01'	(Amount)	(Beløp)	(Amount)	(Beløp)
'02'	(Amount) OK?	Godkjenn (Beløp)	(Amount) OK?	Godkjenn (Beløp)
'03'	Approved	Godkjent	Approved	Godkjent
'04'	Call Your Bank	Kontakt din bank	Call Your Bank	Kontakt din bank
'05'	Cancel or Enter	Slett / Godkjenn	Cancel or Enter	Slett / Godkjenn
'06'	Card Error	Ugyldig kort	Card Error	Ugyldig kort
'07'	Declined	Avvist	Declined	Avvist
'08'	Enter Amount	Tast inn beløp	Enter Amount	Tast inn beløp
'09'	Enter PIN	Tast PIN	Enter PIN	Tast PIN
'0A'	Incorrect PIN	Ugyldig PIN	Incorrect PIN	Ugyldig PIN
'0B'	Insert Card	Sett inn kort	Insert Card	Sett inn kort
'0C'	Not Accepted	Kan ikke anvendes	Not Accepted	Kan ej anvendes
'0D'	PIN OK	PIN OK	PIN OK	PIN OK
'0E'	Please Wait	Vennligst vent	Please Wait	Vennligst vent
'0F'	Processing Error	Teknisk feil	Processing Error	Teknisk feil
'10'	Remove Card	Ta ut kortet	Remove Card	Ta ut kortet
'11'	Use Chip Reader	Bruk chipkortleser	Use Chip Reader	Bruk chipkort
'12'	Use MAG Stripe	Bruk magnetkortleser	Use MAG Stripe	Bruk magnetkort
'13'	Try Again	Prøv igjen	Try Again	Prøv igjen
'14'	Welcome	Velkommen	Welcome	Velkommen
'15'	Present Card	Plassér kortet	Present Card	Plassér kortet
'16'	Processing	Behandler	Processing	Behandler
'17'	Card read OK. Please remove card	Kortet er lest. Fjern kortet	Card read OK. Remove card	Kortet er lest. Fjern kortet
'18'	Please insert or swipe card	Sett inn kort	Please insert or swipe card	Sett inn kort
'19'	Please present one card only	Kun ett kort!	Please present one card only	Kun ett kort!
'1A' – '3F'	RFU for assignment by EMV			
'40'	System Error, retry	Systemfeil	System Error	Systemfeil
'41'	Invalid Card	Ugyldig kort	Invalid Card	Ugyldig kort
'42'	Card out-of-order	Kortet virker ikke	Error in card	Kortet virker ej
'43'	Expired Card	Kort utløpt	Expired Card	Kort utløpt
'44'	Insufficient value	For lav verdi	Too low value	For lav verdi
'45'	Card not present	Kort ikke tilstede	Card missing	Kort ej tilstede
'46'	Data Store full	Datalager fullt	Data Store full	Datalager fullt
'47'	Timed out	Time out	Timed out	Time out
'48'	Thank You	Takk!	Thank You	Takk!
'49'	Not available	Ikke tilgjengelig	Not available	Ej tilgjengelig

Table 1-15.11 - Messages for Display (Norwegian) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Norwegian	English	Norwegian
'4A'	Print receipt?	Ønskes kvittering?	Print receipt?	Kvittering?
'4B'	Cancel	Annuller	Cancel	Annuller
'4C'	Make Selection	Velg	Make Selection	Velg
'4D'	Incorrect Amount	Ugyldig beløp	Wrong Amount	Ugyldig beløp
'4E'	Welcome	Velkommen	Welcome	Velkommen
'4F'	Signature	Underskrift	Signature	Underskrift
'50'	Application Menu	Meny	Menu	Meny
'51'	Transaction Menu	Meny	Menu	Meny
'52'	Purchase	Kjøp	Purchase	Kjøp
'53'	Page	Side	Page	Side
'54'	PIN Blocked	PIN sperret	PIN Blocked	PIN sperret
'55'	Enter New PIN	Tast inn ny PIN	Enter New PIN	Tast inn ny PIN
'56'	PIN Changed	PIN er endret	PIN Changed	PIN er endret
'57'	PIN Unchanged	PIN uendret	PIN Unchanged	PIN uendret
'58'	2 PINs not same	2 PINs ikke like	2 PINs not same	2 PINs ikke like
'59'	Confirm new PIN	Bekreft ny PIN	Confirm new PIN	Bekreft ny PIN
'5A'	Change PIN	Endre PIN	Change PIN	Endre PIN
'5B'	Unblock PIN	Opphev sperret PIN	Unblock PIN	Opph.sperret PIN
'5C'	PIN not blocked	PIN ikke sperret	PIN not blocked	PIN ikke sperret
'5D'	PIN Unblocked	PIN frigjort	PIN Unblocked	PIN frigjort
'5E'	Calling...	Ringer opp...	Calling...	Ringer opp...
'5F'	Transmitting...	Sender...	Transmitting...	Sender...
'60'	Receiving...	Mottager...	Receiving...	Mottager...
'61'	Comms Error	Kommunikasjonsfeil	Comms Error	Kommunik. feil
'62'	Disconnecting	Avbryter	Disconnecting	Avbryter
'63'	Trans Log Upload	Trans. log sendes	Trans Log Upload	Trans. log send.
'64'	Retrying	Prøver igjen	Retrying	Prøver igjen
'65'	Upload Done	Opplastning OK	Upload Done	Opplastning OK
'66'	Upload Failed	Opplastn. mislyktes	Upload Failed	Oppl. mislyktes
'67'	No Records	Ingen data	No Records	Ingen data
'68'	Debit:	Debet:	Debit:	Debet:
'69'	Credit:	Kredit:	Credit:	Kredit:
'6A'	Credit Reversal	Kreditt tilbakefør.	Credit Reversal	Kreditt tilbakef
'6B'	Cash Load	Kontant opplastning	Cash Load	Kontant opplast.
'6C'	Balance:	Saldo:	Balance:	Saldo:
'6D'	New Balance	Ny saldo:	New Balance	Ny saldo:
'6E'	Specify Amount	Angi beløp:	Specify Amount	Angi beløp:
'6F'	Recovery Needed	Rett feil	Recovery Needed	Rett feil
'70'	Insufficient Funds	Beløp for høyt	Value too high	Beløp for høyt

Table 1-15.11 - Messages for Display (Norwegian) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Norwegian	English	Norwegian
'71'	Recovery Failed	Feil ikke rettet	Recovery Failed	Feil ikke rettet
'72'	Recovery Done	Rettelse av feil OK	Recovery Done	Rettelse OK
'73'	Money Taken	Beløp er belastet	Money Taken	Beløp belastet
'74'	Show Balance	Vis saldo	Show Balance	Vis saldo
'75'	Statement Review	Vis kontobalanse	Statement Review	Vis kontobalanse
'76'	by issuer	av utsteder	by issuer	av utsteder
'77'	Upload Time	Opplastningstid	Upload Time	Opplastningstid
'78'	Start (HH:MM)	Start(tt:mm)	Start (HH:MM)	Start(tt:mm)
'79'	End (HH:MM)	Slut(tt:mm)	End (HH:MM)	Slut(tt:mm)
'7A'	Prefix No	Prefiks nr.	Prefix No	Prefiks nr.
'7B'	Totals	Totalt	Totals	Totalt
'7C'	Auth X25 No	Auth. X.25 Nr	Auth X25 No	Auth. X.25 Nr
'7D'	Upload X25 No	Avsender X.25 Nr	Upload X25 No	Avsender X.25 Nr
'7E'	No Trials:	Nr forsøk:	No Trials:	Nr forsøk:
'7F'	Delay:	Forsinkelse:	Delay:	Forsinkelse:
'80'	Online Auth. Data	Online auth. data	Onl Auth. Data	Online auth.data
'81'	Online Upload Data	Online batch data	Onl Upload Data	Onl. batch data
'82'	Get Cash	Kontantuttak	Get Cash	Kontantuttak
'83'	Unblock Appli.	Fjern appl. sperring	Unblock Appli.	Fjern appl.sper.
'84'	Pre-Autho.	Pre-autorisasjon	Pre-Autho.	Pre-autorisasjon
'85'	Pre Completion	Foreløpig avslutning	Pre Completion	Foreløpig avslut
'86'	Refund:	Retur:	Refund:	Retur:
'87'	Cancellation	Annullering	Cancellation	Annullering
'88'	D/C Menu	D/K meny	D/C Menu	D/K meny
'89'	Precomp. Number	Beregn nummer	Precomp. Number	Beregn nummer
'8A'	Get Merchant PIN	Forretnings PIN	Get Merchant PIN	Forretnings PIN
'8B'	Need data in the DB	Data kreves i base	Need data in DB	Data kreves i DB
'8C'	Interval (MM)	Intervall (mm)	Interval (MM)	Intervall (mm)
'8D'	Number Attempts	Antall forsøk	Number Attempts	Antall forsøk
'8E'	Load Stop List	Load sperreliste	Load Stop List	Load sperreliste
'8F'	Pick up Card	Sperret – inndra	Pick up Card	Sperret – inndra
'90'	Denied:	Avvist:	Denied:	Avvist:
'91'	View Balance?	Se saldo?	View Balance?	Se saldo?
'92'	Do not honor	Avvist	Do not honor	Avvist
'93'	Expired Card	Kort utløpt	Expired Card	Kort utløpt
'94'	Suspected fraud	Mulig svindel	Suspected fraud	Mulig svindel
'95'	PIN exceeded	For mange PIN forsøk	PIN exceeded	PIN sperret
'96'	Refer Issuer	Kontakt kortutsteder	Refer Issuer	Kontakt kortutsteder

Table 1-15.11 - Messages for Display (Norwegian) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Norwegian	English	Norwegian
'97'	No card number	Ingen kortnr	No card number	Ingen kortnr
'98'	Excessive Amount	For høyt beløp	Excessive Amount	For høyt beløp
'99'	Counterfeit Card	Falskt kort	Counterfeit Card	Falskt kort
'9A'	Format Error	Formatfeil	Format Error	Formatfeil
'9B'	Card issuer or	Kortutsteder eller	Card issuer or	Kortutsteder el.
'9C'	Switch inop.	Switch ute av drift	Switch inop.	Switch feiler
'9D'	Bad Routing	Bad routing	Bad Routing	Bad routing
'9E'	Sys malfunction	Systemfeil	Sys malfunction	Systemfeil
'9F'	Yes	Ja	Yes	Ja
'A0'	No	Nei	No	Nei
'A1'	Capture Card	Inndra kort	Capture Card	Inndra kort
'A2'	Money not taken	Beløp ikke trukket	Money not taken	Beløp ej trukket
'A3'	Exp. date (YYMM)	Utløpsdato (ÅÅMM)	Exp. date (YYMM)	Utløpsdato(ÅÅMM)
'A4'	Enter PAN	Tast inn kortnr.	Enter PAN	Tast inn kortnr.
'A5'	Enter Term ID	Tast inn terminal ID	Enter Term ID	Tast inn term.ID
'A6'	Params Required	Parametre kreves	Params Required	Parametre kreves
'A7'	Forced online	Online kreves	Forced online	Online kreves
'A8'	Sale:	Salg:	Sale:	Salg:
'A9'	Refund:	Tilbakebetaling:	Refund:	Tilbakebetaling:
'AA'	Purse empty	Pungen er tom	Purse empty	Pungen er tom
'AB'	Set currency	Angi valuta	Set currency	Angi valuta
'AC'	Currency changed	Valutakode endret	Currency changed	Valutakode endret
'AD'	Terminal ID	Terminal ID	Terminal ID	Terminal ID
'AE'	Exceeds limit	Grense overskredet	Exceeds limit	Over grense
'AF'	Invalid currency	Ugyldig valuta	Invalid currency	Ugyldig valuta
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	Terminalen er klar	Terminal ready	Terminalen klar
'E1' 1)	No receipt	Ingen kvittering	No receipt	Ingen kvittering
'E2'				
'E3'	Error reading card	Feil med kort	Card read error	Feil med kort
'E4'	Card validated	Kort godkjent	Card validated	Kort godkjent
'E5'	Receipt wanted?	Ønskes kvittering?	Receipt wanted?	Ønskes kvitter?
'E6'	Printing receipt	Kvittering skrives ut	Printing receipt	Kvitt. skrives ut
'E7'	Purchase interrupted	Kjøpet er avbrutt	Purchase stopped	Kjøpet avbrutt
'E8'	Terminal failure	Feil i terminalen	Terminal failure	Feil i terminal
'E9'	Terminal busy	Terminal er opptatt	Terminal busy	Terminal opptatt
'EA'	Out of order	Ute av drift	Out of order	Ute av drift
'EB'	Push	Trykk	Push	Trykk
'EC'	Enter PIN and Accept	Tast PIN og Godkjenn	Enter PIN/Accept	Tast PIN/Godkj.

Table 1-15.11 - Messages for Display (Norwegian) (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	Norwegian	English	Norwegian
'ED'	Swipe card	Trekk kort	Swipe card	Trekk kort
'EE'	Insert card again	Sett inn kort igjen	Insert card	Sett inn kort
'EF'	PIN:	PIN:	PIN:	PIN:
'F0'	Buy:	Kjøp:	Buy:	Kjøp:
'F1'	Accept?	Tast Godkjenn	Accept?	Tast Godkjenn
'F2'	Bonus added	Bonus registrert	Bonus added	Bonus registrert
'F3'	Technical failure	Teknisk feil	Tech. failure	Teknisk feil
'F4'	Try again later	Prøv igjen senere	Try again later	Prøv senere
'F5'	Limit reached	Over max. grense	Limit reached	Over max. grense
'F6'	Card is blocked	Kort er sperret	Card is blocked	Kort er sperret
'F7'	Refer Acquirer	Ring innløser	Refer Acquirer	Ring innløser
'F8'	(X) PIN tries left	(X) PIN forsøk igjen	(X) PIN try left	(X) PIN fors.
'F9'	Invalid merchant	Ukjent forretning	Invalid merchant	Ukjent forretn.
'FA'	Card unknown	Kortet er ukjent	Card unknown	Kortet er ukjent
'FB'	Split payment?	Delt betaling?	Split payment?	Delt betaling?
'FC'	Card/amount recorded	Kort/beløp notert	Data recorded	Kort/beløp not.
'FD'	Identical purchase	Identisk kjøp utført	Identical trans.	Identisk kjøp
'FE'	(Action Code)	(Action Code)	(Action Code)	(Action Code)
'FF'	Invalid transaction	Ugyldig transaksjon	Invalid trans.	Ugyldig transak.

Legend: ¹⁾ The message may flash on the display to attract the cardholder's attention.
²⁾ A “-” or a “+” may be used instead of the “/”.
Generally, when “(“and”) are used, the actual value of whatever is inside the brackets is indicated.
(X) indicates actual value.
Message Codes 'EC' and 'F1' are proposed text

1-15.4.3 Receipt Texts

- 1-15.4.3.1 A Below is table 1-15.13 that defines the regional Norwegian texts that shall be used when printing receipts.

Table 1-15.12 - Messages for Printing (Norwegian)

Receipt Line	Element	English	Norwegian
'MI4'	Phone	Phone:	TLF:
'MI5'	Business Reg. number	Buss.Reg.No:	Org. Nr.
'HI2'	Copy indicator	Copy	Kopi
'HI4a'	Prelim/post indicator	Preliminary	Foreløpig
'HI4b'	Prelim/post indicator	Post registration	Etterregistrering
'HI4c'	Cancellation indicator	Cancellation	Annullering
'HI5'	Non-financial indicator	This is not a receipt	Ikke gyldig kvittering

Table 1-15.13 - Messages for Printing (Norwegian) (*continued*)

Receipt Line	Element	English	Norwegian
'HI7a'	Transaction indicator	Authorization only	Kun autorisasjon
'HI7b'		Refund	Retur
'HI7c'		Reversal (auth)	Annullering (Aut.)
'HI7d'		Cancellation	Kansellering
'HI7e'		Cash	Kontanter
'AM2a'	Amount type	Purchase	Kjøp
'AM2b'		Refund	Retur
'AM2c'		Cash	Kontanter
'AM2d'		Amount	Beløp
'AM4'	V.A.T.	VAT incl.	Herav moms
'AM5'	Surcharge	Surcharge	Gebyr
'AM6'	Cashback	Cashback	Kontantuttak
'AM7' / 'AM11'	Extra	Extra	Ekstra
'AM9' / 'AM13'	Total	Total	Total
'TR1'	PIN indicator	PIN used	PIN benyttet
'TR3'	Payment code	Paym.code:	Betalingskode
'TR4a'	Account type	Saving transaction	<Not Applicable>
'TR4b'		Debit transaction	<Not Applicable>
'TR4c'		Credit transaction	<Not Applicable>
'TR8'	Merchant number	Me.No:	Nets nr.
'TR12'	Status	Status:	Status:
'TR13'	Auth.code	Auth.code:	Aut. kode:
'TR14'	Auth.result	Authorized	Autorisert
'SI2/SI4'	Tips info – 1	** When tipping **	** Ved ekstra **
'SI3/SI5'	Tips info –2	Ask for new receipt	Husk ny kvittering
'SI6/SI7'a	Approval message	Approved for \ crediting of account	Beløp godkjennes
'SI6/SI7'b		Approved for debiting\ of account as above	Beløp godkjennes
'SI8'	Card reference	Printed digits:	Trykte tall:
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	Identifikasjon:
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	Utstedt af:
'SI16'	ID expiry date	ID expiry date:	ID utløpsdato:
'SI18'	Clerk ID	Clerk ID:	Operatør ID:
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholders account by the issuer	Gebyr kan blive til- føjet af kortutsteder
'SI26'a	Signatory type	Merchant's signature	Forretningens signatur
'SI26'b		Cardholders signature	Kortholders signatur

Table 1-15.13 - Messages for Printing (Norwegian) (*concluded*)

Receipt Line	Element	English	Norwegian
'FI2'a	Termination reason	Interrupted – cancel	Avbrutt – kansellér
'FI2'b		Declined	Avvist
'FI2'c		Signature declined	Signatur avvist
'FI2'd		Interrupted – error	Avbrutt – feil
'FI7'		Retain receipt	Behold kvittering
'FI8'a	Recipient indicator	Cardholders' receipt	Kortholders kopi
'FI8'b		Merchant's receipt	Brukerstedets kopi
'PC3'	Balance amount	Balance	Saldo
'PC4'	Expiry date	Exp.date	Utløpsdato

1-15.5 Finland

1-15.5.1 Functional Requirements

Additional card and terminal data

- 1-15.5.1.1 A A Finnish terminal will, when performing transactions using ICC's, include the following additional data in tags in field 55;
- 9F09, b2, Application Version Number,
 - 9F1E, b8, Interface Device (reader) Serial Number,
 - 9F35, b1, Terminal Type,
 - 9F53, b1, Trans Category Code

NOTE: This is handled by the PSAM.

NOTE: The host will take the data returned as tag '4F' and re-name it to tag '84'.

- 1-15.5.1.2 A A Finnish terminal shall for each transaction, include the following additional data tags;
- 6J, an2, Finnish Terminal Supplier,
 - 6K, an1, Finnish Terminal Type,
 - 6R, an1, Permanent Terminal Type,
 - UQ, n20, Finnish Payment Reference

- 1-15.5.1.3 A The data shall be transferred to the PSAM using the call *Set Debit/Credit Properties* with an identifier of 8004. See 2-14.42 for further details.

NOTE: The Finnish infrastructure does not support Online PIN, whereas certain international brands require Online PIN. Finnish terminal may be set up to enable Online PIN for these BIN's despite the Terminal is **not** supporting Online PIN in general.

Language selection

- 1-15.5.1.4 A A terminal to be used in Finland shall at least be able to use Finnish and Swedish as language.

1-15.5.2 Display Texts

- 1-15.5.2.1 A Table 1-15.14 defines the regional texts that shall be used when displaying text in Finnish.
- 1-15.5.2.2 A Table 1-15.9 defines the regional texts that shall be used when displaying text in Swedish.

Table 1-15.14 - Messages for Display (Finnish)

Message Code	20 Characters Display		16 Characters Display	
	English	Finnish	English	Finnish
'01'	(Amount)	(Amount) (Cur.Code)	(Amount)	(Amnt)(Cur.Code)
'02'	(Amount) OK?	(Amnt)(Cur.Code)OK?	(Amount) OK?	(AC) OK?
'03'	Approved	Hyväksytty	Approved	Hyväksytty
'04'	Call Your Bank	Soita pankkiin	Call Your Bank	Soita pankkiin
'05'	Cancel or Enter	Peruuta tai hyväksy	Cancel or Enter	Peruuta/hyväksy
'06'	Card Error	Korttivirhe	Card Error	Korttivirhe
'07'	Declined	Hylätty	Declined	Hylätty
'08'	Enter Amount	Syötä summa	Enter Amount	Syötä summa
'09'	Enter PIN	Syötä PIN	Enter PIN	Syötä PIN
'0A'	Incorrect PIN	PIN virheellinen	Incorrect PIN	PIN virheellinen
'0B'	Insert Card	Syötä kortti	Insert Card	Syötä kortti
'0C'	Not Accepted	Ei hyväksytty	Not Accepted	Ei hyväksytty
'0D'	PIN OK	PIN OK	PIN OK	PIN OK
'0E'	Please Wait	Odota, ole hyvä	Please Wait	Odota, ole hyvä
'0F'	Processing Error	Käsittelyvirhe	Processing Error	Käsittelyvirhe
'10'	Remove Card	Poista kortti	Remove Card	Poista kortti
'11'	Use Chip Reader	Käytä sirulukijaa	Use Chip Reader	Käytä siruluk.
'12'	Use MAG Stripe	Käytä mg-juovaa	Use MAG Stripe	Käytä mg-juovaa
'13'	Try Again	Yritä uudelleen	Try Again	Yritä uudelleen
'14'	Welcome	Tervetuloa	Welcome	Tervetuloa
'15'	Present Card	Anna kortti	Present Card	Anna kortti
'16'	Processing	Käsittelee	Processing	Käsittelee
'17'	Card read OK. Please remove card	Kortti luettu Ota kortti	Card read OK. Remove card	Kortti luettu. Ota kortti.
'18'	Please insert or swipe card	Syötä kortti	Please insert or swipe card	Syötä kortti
'19'	Please present one card only	Vain yksi kortti	Please present one card only	Vain yksi kortti
'1A' – '3F'	RFU for assignment by EMV			
'40'	System Error, retry	Virhe, yritä uud.	System Error	Virhe,yritä uud.
'41'	Invalid Card	Kortti virheellinen	Invalid Card	Virh. kortti
'42'	Card out-of-order	Kortti vioittunut	Error in card	Viallinen kortti
'43'	Expired Card	Kortti vanhentunut	Expired Card	Kortti vanh.
'44'	Insufficient value	Ei riittävästi varoja	Too low value	Ei varoja
'45'	Card not present	Ei korttia	Card missing	Ei korttia
'46'	Data Store full	Muisi täynnä	Data Store full	Muisi täynnä
'47'	Timed out	Time-out!	Timed out	Time-out!
'48'	Thank You	Kiitos	Thank You	Kiitos
'49'	Not available	Ei käytettävissä	Not available	Ei käytettävissä
'4A'	Print receipt?	Tulosta kuitti?	Print receipt?	Tulosta kuitti?

Table 1-15.14 - Messages for Display (Finnish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Finnish	English	Finnish
'4B'	Cancel	Peruuta	Cancel	Peruuta
'4C'	Make Selection	Valitse	Make Selection	Valitse
'4D'	Incorrect Amount	Summa virheellinen	Wrong Amount	Virheell.summa
'4E'	Welcome	Tervetuloa	Welcome	Tervetuloa
'4F'	Signature	Allekirjoitus	Signature	Allekirjoitus
'50'	Application Menu	Sovellusvalikko	Menu	Valikko
'51'	Transaction Menu	Tapahtumavalikko	Menu	Valikko
'52'	Purchase	Veloitus	Purchase	Veloitus
'53'	Page	Sivu	Page	Sivu
'54'	PIN Blocked	PIN estetty	PIN Blocked	PIN estetty
'55'	Enter New PIN	Syötä uusi PIN	Enter New PIN	Syötä uusi PIN
'56'	PIN Changed	PIN vaihdettu	PIN Changed	PIN vaihdettu
'57'	PIN Unchanged	PINiä ei vaihdettu	PIN Unchanged	PIN ei vaihdettu
'58'	2 PINs not same	PINit eivät täsmää	2 PINs not same	2 eri PINiä
'59'	Confirm new PIN	Vahvista uusi PIN	Confirm new PIN	Vahvista PIN
'5A'	Change PIN	Vaihda PIN	Change PIN	Vaihda PIN
'5B'	Unblock PIN	Vapauta PIN	Unblock PIN	Vapauta PIN
'5C'	PIN not blocked	PINiä ei estetty	PIN not blocked	PINiä ei estetty
'5D'	PIN Unblocked	PIN vapautettu	PIN Unblocked	PIN vapautettu
'5E'	Calling...	Soittaa..	Calling...	Soittaa..
'5F'	Transmitting...	Lähetää..	Transmitting...	Lähetää..
'60'	Receiving...	Vastaanottaa..	Receiving...	Vastaanottaa..
'61'	Comms Error	Yhteysvirhe	Comms Error	Yhteysvirhe
'62'	Disconnecting	Yhteyden katkaisu	Disconnecting	Yht.katkaisu
'63'	Trans Log Upload	Tapahtumaloki	Trans Log Upload	Tapahtumaloki
'64'	Retrying	Uudelleenyritys	Retrying	Uudelleenyritys
'65'	Upload Done	Siirto valmis	Upload Done	Siirto valmis
'66'	Upload Failed	Siirto epäonnistui	Upload Failed	Siirto epäonn.
'67'	No Records	Ei tietoja	No Records	Ei tietoja
'68'	Debit:	Veloitus:	Debit:	Veloitus:
'69'	Credit:	Hyvitys:	Credit:	Hyvitys:
'6A'	Credit Reversal	Hyvityksen peruutus	Credit Reversal	Hyvityksen per.
'6B'	Cash Load	Lataa arvo	Cash Load	Lataa arvo
'6C'	Balance:	Saldo:	Balance:	Saldo:
'6D'	New Balance	Uusi saldo	New Balance	Uusi saldo
'6E'	Specify Amount	Määritä summa	Specify Amount	Määritä summa
'6F'	Recovery Needed	Tekninen virhe	Recovery Needed	Tekninen virhe
'70'	Insufficient Funds	Puutteellinen arvo	Value too high	Liian suuri arvo
'71'	Recovery Failed	Palautus epäonnistui	Recovery Failed	Palautus epäonn.

Table 1-15.14 - Messages for Display (Finnish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Finnish	English	Finnish
'72'	Recovery Done	Palautus onnistui	Recovery Done	Palautus onn.
'73'	Money Taken	Veloitettu	Money Taken	Veloitettu
'74'	Show Balance	Näytä saldo	Show Balance	Näytä saldo
'75'	Statement Review	Tapahtumat	Statement Review	Tapahtumat
'76'	by issuer	kortinmyöntäjältä	by issuer	kortinmyöntäjä
'77'	Upload Time	Siirtoaika	Upload Time	Siirtoaika
'78'	Start (HH:MM)	Alkaa (HH:MM)	Start (HH:MM)	Alkaa (HH:MM)
'79'	End (HH:MM)	Päätyy (HH:MM)	End (HH:MM)	Päätyy (HH:MM)
'7A'	Prefix No	Kortin BIN	Prefix No	Kortin BIN
'7B'	Totals	Yhteensä	Totals	Yhteensä
'7C'	Auth X25 No	Varm. X25 nro	Auth X25 No	Varm. X25 nro
'7D'	Upload X25 No	Siirto X25 nro	Upload X25 No	Siirto X25 nro
'7E'	No Trials:	Ei yrityksiä:	No Trials:	Ei yrityksiä:
'7F'	Delay:	Viive:	Delay:	Viive:
'80'	Onl Auth. Data	Varm. tiedot	Onl Auth. Data	Varm.tiedot
'81'	Onl Upload Data	Siirtotiedot	Onl Upload Data	Siirtotiedot
'82'	Get Cash	Käteisnosto	Get Cash	Käteisnosto
'83'	Unblock Appli.	Vapauta sovellus	Unblock Appli.	Vapauta sovellus
'84'	Pre-Autho.	Ennakkovarmennus	Pre-Autho.	Ennakkovarm.
'85'	Pre Completion	Ennakkovahvistus	Pre Completion	Ennakkovahv.
'86'	Refund:	Palautus:	Refund:	Palautus:
'87'	Cancellation	Peruutus	Cancellation	Peruutus
'88'	D/C Menu	D/C Valikko	D/C Menu	D/C Valikko
'89'	Precomp. Number	Ennakkovahv. nro	Precomp. Number	Ennakkovahv. nro
'8A'	Get Merchant PIN	Kauppiasnumero	Get Merchant PIN	Kauppiasnumero
'8B'	Data required in the DB	Tietokanta-aineisto	Need data in DB	TK aineisto
'8C'	Interval (MM)	Väli (MM)	Interval (MM)	Väli (MM)
'8D'	Number Attempts	Yritysten määrä	Number Attempts	Yritysten määrä
'8E'	Load Stop List	Lataa sulkulista	Load Stop List	Lataa sulkulista
'8F'	Pick up Card	Takavarikoi kortti	Pick up Card	Takavar. kortti
'90'	Denied:	Hylätty:	Denied:	Hylätty:
'91'	View Balance?	Tarkasta saldo?	View Balance?	Tarkasta saldo?
'92'	Do not honor	Älä huomioi	Do not honor	Älä huomioi
'93'	Expired Card	Kortti vanhentunut	Expired Card	Kortti vanh.
'94'	Suspected fraud	Petosepäily	Suspected fraud	Petosepäily
'95'	PIN exceeded	Liian pitkä PIN	PIN exceeded	Liian pitkä PIN
'96'	Refer Issuer	Ota yht. myöntäjään	Refer Issuer	Yht.myöntäjään
'97'	No card number	Ei korttinumeroa	No card number	Ei korttinumeroa

Table 1-15.14 - Messages for Display (Finnish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Finnish	English	Finnish
'98'	Excessive Amount	Liian suuri summa	Excessive Amount	Liian paljon
'99'	Counterfeit Card	Väärennetty kortti	Counterfeit Card	Korttiväärennös
'9A'	Format Error	Väärä muoto	Format Error	Väärä muoto
'9B'	Card issuer or	Kortinmyöntäjä tai	Card issuer or	Myöntäjä tai
'9C'	Switch inop.	Ei yhteyttä	Switch inop.	Ei yhteyttä
'9D'	Bad Routing	Reitiysongelma	Bad Routing	Reitiysongelma
'9E'	Sys malfunction	Järjestelmävirhe	Sys malfunction	Järjestelmävirhe
'9F'	Yes	Kyllä	Yes	Kyllä
'A0'	No	Ei	No	Ei
'A1'	Capture Card	Ota kortti pois	Capture Card	Ota kortti pois
'A2'	Money not taken	Ei veloitettu	Money not taken	Ei veloitettu
'A3'	Exp. date (YYMM)	Voimassa (VVKK) asti	Exp. date (YYMM)	Voim.(VVKK) asti
'A4'	Enter PAN	Syötä korttinumero	Enter PAN	Syötä korttinro.
'A5'	Enter Term ID	Syötä päätetunnus	Enter Term ID	Syötä päätetunn.
'A6'	Params Required	Parametriasetukset	Params Required	Param.asetukset
'A7'	Forced online	Pakotettu yhteys	Forced online	Pakotettu yhteys
'A8'	Sale:	Myynti:	Sale:	Myynti:
'A9'	Refund:	Palautus:	Refund:	Palautus:
'AA'	Purse empty		Purse empty	
'AB'	Set currency	Anna arvo	Set currency	Anna arvo
'AC'	Currency changed	Aseta valuutta	Currency changed	Aseta valuutta
'AD'	Terminal ID	Päätetunnus	Terminal ID	Päätetunnus
'AE'	Exceeds limit	Ylittää rajan	Exceeds limit	Ylittää rajan
'AF'	Invalid currency	Virheell. valuutta	Invalid currency	Virh. valuutta
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	Pääte valmis	Terminal ready	Pääte valmis
'E1' 1)	No receipt	Ei kuittia	No receipt	Ei kuittia
'E2'				
'E3'	Error reading card	Kortinlukuvirhe	Card read error	Kortinlukuvirhe
'E4'	Card validated	Kortti hyväksytty	Card validated	Kortti hyv.
'E5'	Receipt wanted?	Haluatko kuitin?	Receipt wanted?	Haluatko kuitin?
'E6'	Printing receipt	Kuitin tulostus	Printing receipt	Kuitin tulostus
'E7'	Purchase interrupted	Osto keskeytetty	Purchase stopped	Osto keskeytetty
'E8'	Terminal failure	Päätteen virhe	Terminal failure	Päätteen virhe
'E9'	Terminal busy	Pääte varattu	Terminal busy	Pääte varattu
'EA'	Out of order	Epäkunnossa	Out of order	Epäkunnossa
'EB'	Push	Työnnä	Push	Työnnä
'EC'	Enter PIN and Accept	Syötä PIN ja hyväksy	Enter PIN/Accept	PIN/hyväksyntä

Table 1-15.14 - Messages for Display (Finnish) (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	Finnish	English	Finnish
'ED'	Swipe card	Lue kortti	Swipe card	Lue kortti
'EE'	Insert card again	Aseta kortti uudell.	Insert card	Kortti uudelleen
'EF'	PIN:	PIN:	PIN:	PIN:
'F0'	Buy:	Osto:	Buy:	Osto:
'F1'	Accept?	Hyväksy?	Accept?	Hyväksy?
'F2'	Bonus added	Bonus lisätty	Bonus added	Bonus lisätty
'F3'	Technical failure	Tekninen virhe	Tech. failure	Tekninen virhe
'F4'	Try again later	Yritä myöh.uudelleen	Try again later	Yritä uudelleen
'F5'	Limit reached	Uli max. Rajan	Limit reached	Uli max. Rajan
'F6'	Card is blocked	Kortti estetty	Card is blocked	Kortti estetty
'F7'	Refer Acquirer	Yht. Kortinantajaan	Refer Acquirer	Yht. K-antajaan
'F8'	(X) PIN tries left	PIN-yrityksiä:(X)	(X) PIN tries left	PIN-syötöt:(X)
'F9'	Invalid merchant	Virh. kauppias	Invalid merchant	Virh. kauppias
'FA'	Card unknown	Tuntematon kortti	Card unknown	Tuntem.kortti
'FB'	Split payment?	Jaa maksu?	Split payment?	Jaa maksu?
'FC'	Card/amount recorded	Kortti/summa rekist.	Data recorded	Kortti/summa OK
'FD'	Identical purchase	Sama tapahtuma	Identical trans.	Sama tapahtuma
'FE'	(Action Code)	(Action Code)	(Action Code)	(Action Code)
'FF'	Invalid transaction	Virhe tapahtumassa	Invalid trans.	Virh.tapahtuma

Legend: ¹⁾ The message may flash on the display to attract the cardholder's attention.
²⁾ A "-" or a "+" may be used instead of the "/".
Generally, when "("and") are used, the actual value of whatever is inside the brackets is indicated.
(X) indicates actual value.
Message Codes 'EC' and 'F1' are proposed text

1-15.5.3 Receipt Texts

- 1-15.5.3.1 A Table 1-15.15 defines the regional texts that shall be used when printing receipts in Finnish.
- 1-15.5.3.2 A Table 1-15.10 defines the regional texts that shall be used when printing receipts in Swedish.

Table 1-15.15 - Messages for Printing (Finnish)

Receipt Line	Element	English	Finnish
'MI4'	Phone	Phone:	
'MI5'	Business Reg. number	Bus.Reg.No:	Y-Tunnus:
'HI2'	Copy indicator	Copy	Kopio
'HI4a'	Prelim/post indicator	Preliminary	Alustava
'HI4b'	Prelim/post indicator	Post registration	Jälkirekisteröinti
'HI4c'	Cancellation indicator	Cancellation	Peruutus
'HI5'	Non-financial indicator	This is not a receipt	Ei kuitti ostosta
'HI7a'	Transaction indicator	Authorization only	Vain Varmennus
'HI7b'		Refund	Hyvitys
'HI7c'		Reversal (auth)	Peruutus (varm)
'HI7d'		Cancellation	Peruutus
'HI7e'		Cash	Käteinen
'AM2a'	Amount type	Purchase	Osto
'AM2b'		Refund	Hyvitus
'AM2c'		Cash	Käteinen
'AM2d'		Amount	Summa
'AM4'	V.A.T.	VAT incl.	Alv
'AM5'	Surcharge	Surcharge	Provisio
'AM6'	Cashback	Cashback	Käteisnosto
'AM7' / 'AM11'	Extra	Extra	Ekstra
'AM9' / 'AM13'	Total	Total	Yhteensä
'TR1'	PIN indicator	PIN used	PIN syötetty
'TR3'	Payment code	Paym.code:	Kauppiaskoodi
'TR4a'	Account type	Saving transaction	<blank>
'TR4b'		Debit transaction	Debit
'TR4c'		Credit transaction	Credit
'TR8'	Merchant number	Me.No:	Nets nro.
'TR12'	Status	Status:	Status:
'TR12'	Auth.code	Auth.code:	Auth. Code:
'TR14'	Auth.result	Authorized	Authorized
'SI2/SI4'	Tips info – 1	** When tipping **	**tipin yhteydessä**
'SI3/SI5'	Tips info –2	Ask for new receipt	Muista uusi kuitti

Table 1-15.15 - Messages for Printing (Finnish) (*concluded*)

Receipt Line	Element	English	Finnish
'SI6/SI7'a	Approval message	Approved for \ crediting of account	
'SI6/SI7'b		Approved for debiting\ of account as above	
'SI8'	Card reference	Printed digits:	Tulostetut numerot:
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	Tunnistus: (Passi tms.)
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	
'SI16'	ID expiry date	ID expiry date:	
'SI18'	Clerk ID	Clerk ID:	Myyjänumero
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholders account by the issuer	
'SI26'a	Signatory type	Merchant's signature	Kauppiaan allekirjoitus
'SI26'b		Cardholders signature	Kortinhalt. Allekirjoitus
'FI2'a	Termination reason	Interrupted – cancel	Keskeytetty–peruuta
'FI2'b		Declined	Hylätty
'FI2'c		Signature declined	Allekirjoitus hylätty
'FI2'd		Interrupted – error	Allekirjoitus hylätty
'FI7'		Retain receipt	Säilytä kuitti
'FI8'a	Recipient indicator	Cardholders' receipt	Asiakkaan kappale
'FI8'b		Merchant's receipt	Kauppiaan kappale
'PC3'	Balance amount	Balance	Saldo
'PC4'	Expiry date	Exp.date	Voim.olo pvm

1-15.6 Germany

1-15.6.1 Functional Requirements

Nets Denmark A/S is not aware of any specific German requirements not already specified either in this document or in the referenced documents.

1-15.6.2 Display Texts

- 1-15.6.2.1 B Regional texts that shall be used when displaying text where German is the language chosen are defined in table 1-15.16 below.

Table 1-15.16 - Messages for Display (German)

Message Code	20 Characters Display		16 Characters Display	
	English	German	English	German
'01'	(Amount)	(Amount)(Cur.Code)	(Amount)	(Amount)(Cur.Code)
'02'	(Amount) OK?	(Amnt)(Cur.Code) Bestätigen	(Amount) OK?	(Amnt)(Cur.Code) Bestätigen
'03'	Approved	Autorisier. erfolgt	Approved	Autoris. erfolgt
'04'	Call Your Bank	Bitte Bank kontakt.	Call Your Bank	Bank kontakt.
'05'	Cancel or Enter	Abbr. / Enter drück.	Cancel or Enter	Abbr./Ent.drück.
'06'	Card Error	Kartenfehler	Card Error	Kartenfehler
'07'	Declined	Abgelehnt	Declined	Abgelehnt
'08'	Enter Amount	Betrag eingeben	Enter Amount	Betrag eingeben
'09'	Enter PIN	Bitte PIN eingeben	Enter PIN	PIN eingeben
'0A'	Incorrect PIN	PIN falsch	Incorrect PIN	PIN falsch
'0B'	Insert Card	Karte einstecken	Insert Card	Karte einstecken
'0C'	Not Accepted	Vorgang nicht mögl.	Not Accepted	Vorg.nicht mögl.
'0D'	PIN OK	PIN korrekt	PIN OK	PIN korrekt
'0E'	Please Wait	Bitte warten	Please Wait	Bitte warten
'0F'	Processing Error	Vorgang abgebrochen	Processing Error	Vorg. abgebrochen
'10'	Remove Card	Bitte Karte entnehmen	Remove Card	Karte entnehmen
'11'	Use Chip Reader	Chipleser benutzen	Use Chip Reader	Chip benutzen
'12'	Use MAG Stripe	Mag. streifen verw.	Use MAG Stripe	Mag.streif.verw.
'13'	Try Again	Neue Eingabe	Try Again	Neue Eingabe
'14'	Welcome	Willkommen	Welcome	Willkommen
'15'	Present Card		Present Card	
'16'	Processing	Verarbeitend	Processing	Verarbeitend
'17'	Card read OK. Please remove card		Card read OK. Remove card	
'18'	Please insert or swipe card		Please insert or swipe card	
'19'	Please present one card only		Please present one card only	
'1A' – '3F'	RFU for assignment by EMV			

Table 1-15.16 - Messages for Display (German) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	German	English	German
'40'	System Error, retry	Systemfehler	System Error	Systemfehler
'41'	Invalid Card	Karte ungültig	Invalid Card	Karte ungültig
'42'	Card out-of-order	Kartdaten falsch	Error in card	Kartdaten falsch
'43'	Expired Card	Karte verfallen	Expired Card	Karte verfallen
'44'	Insufficient value	Betrag zu gering	Too low value	Betrag zu gering
'45'	Card not present	Karte einstecken	Card missing	Karte einstecken
'46'	Data Store full	Speicher voll	Data Store full	Speicher voll
'47'	Timed out	Timeout!	Timed out	Timeout!
'48'	Thank You	Vielen Dank	Thank You	Vielen Dank
'49'	Not available	Nicht verfügbar	Not available	Nicht verfügbar
'4A'	Print receipt?	Beleg Drucken?	Print receipt?	Beleg Drucken?
'4B'	Cancel	Abbruch	Cancel	Abbruch
'4C'	Make Selection	Bitte wählen	Make Selection	Bitte wählen
'4D'	Incorrect Amount	Falscher Betrag	Wrong Amount	Falscher Betrag
'4E'	Welcome	Willkommen	Welcome	Willkommen
'4F'	Signature	Unterschrift	Signature	Unterschrift
'50'	Application Menu	Applikationsmenü	Menu	Applikationsmenü
'51'	Transaction Menu	Transaktionsmenü	Menu	Transaktionsmenü
'52'	Purchase	Zahlung	Purchase	Zahlung
'53'	Page	Seite	Page	Seite
'54'	PIN Blocked	PIN gesperrt	PIN Blocked	PIN gesperrt
'55'	Enter New PIN	Neue PIN eingeben	Enter New PIN	Neue PIN eingeb.
'56'	PIN Changed	PIN geändert	PIN Changed	PIN geändert
'57'	PIN Unchanged	PIN nicht geändert	PIN Unchanged	PIN nicht geänd.
'58'	2 PINs not same	PINs nicht gleich	2 PINs not same	PIN nicht gleich
'59'	Confirm new PIN	Bestätig. neue PIN	Confirm new PIN	Bestät. neue PIN
'5A'	Change PIN	Ändere PIN	Change PIN	Ändere PIN
'5B'	Unblock PIN	PIN freischalten	Unblock PIN	PIN freischalten
'5C'	PIN not blocked	PIN freigeschaltet	PIN not blocked	PIN freigeschal.
'5D'	PIN Unblocked	PIN nicht gesperrt	PIN Unblocked	PIN nicht gesp.
'5E'	Calling...	Rufen ...	Calling...	Rufen ...
'5F'	Transmitting...	Senden ...	Transmitting...	Senden...
'60'	Receiving...	Empfangen ...	Receiving...	Empfangen ...
'61'	Comms Error	Kommunikationsfehler	Comms Error	Kommunik.-fehler
'62'	Disconnecting	Verbindungsabbau	Disconnecting	Verbindungsabbau
'63'	Trans Log Upload	Translog senden	Trans Log Upload	Translog senden
'64'	Retrying	Wiederholen	Retrying	Wiederholen
'65'	Upload Done	Senden Okay	Upload Done	Senden Okay

Table 1-15.16 - Messages for Display (German) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	German	English	German
'66'	Upload Failed	Fehler beim Senden	Upload Failed	Fehler beim Send
'67'	No Records	Keine Daten	No Records	Keine Daten
'68'	Debit:	Debit:	Debit:	Debit:
'69'	Credit:	Kredit:	Credit:	Kredit:
'6A'	Credit Reversal	Kreditkartenstorno	Credit Reversal	Kreditkarten-\storno
'6B'	Cash Load	Lade Bargeld	Cash Load	Lade Bargeld
'6C'	Balance:	Guthaben:	Balance:	Guthaben:
'6D'	New Balance	Neues Guthaben:	New Balance	Neues Guthaben:
'6E'	Specify Amount	Betrag eingeben	Specify Amount	Betrag eingeben
'6F'	Recovery Needed	Wiederherst. erford.	Recovery Needed	Wiederh. erford.
'70'	Insufficient Funds	Betrag zu hoch	Value too high	Betrag zu hoch
'71'	Recovery Failed	Wiederherst.– fehler	Recovery Failed	Wiederh.– fehler
'72'	Recovery Done	Wiederherst. OK	Recovery Done	Wiederherst. OK
'73'	Money Taken	Betrag gebucht	Money Taken	Betrag gebucht
'74'	Show Balance	Guthaben anzeigen	Show Balance	Guthaben anzeig.
'75'	Statement Review	Kontoanzeige	Statement Review	Kontoanzeige
'76'	by issuer	bei Kartenausgeber	by issuer	bei Kartenausgeb
'77'	Upload Time	Zeit Datentransfer	Upload Time	Zeit Datentrans.
'78'	Start (HH:MM)	Start (tt:mm)	Start (HH:MM)	Start (tt:mm)
'79'	End (HH:MM)	Ende (tt:mm)	End (HH:MM)	Ende (tt:mm)
'7A'	Prefix No	Prefix–Nr.	Prefix No	Prefix–Nr.
'7B'	Totals	Gesamtsumme	Totals	Gesamtsumme
'7C'	Auth X25 No	Aut. X.25 Nr.	Auth X25 No	Aut. X.25 Nr.
'7D'	Upload X25 No	Sende X25 Nr.	Upload X25 No	Sende X25 Nr.
'7E'	No Trials:	Nr Versuche:	No Trials:	Nr Versuche:
'7F'	Delay:	Verzögerung:	Delay:	Verzögerung:
'80'	Onl Auth. Data	Sende Trxns Daten	Onl Auth. Data	Sende Trns Daten
'81'	Onl Upload Data	Sende Daten	Onl Upload Data	Sende Daten
'82'	Get Cash	Zahlung mit Bargeld	Get Cash	Zahl.mit Bargeld
'83'	Unblock Appli.	Applik freischalten	Unblock Appli.	App freischalten
'84'	Pre–Autho.	Reservierung	Pre–Autho.	Reservierung
'85'	Pre Completion	Vorautorisierung	Pre Completion	Vorautorisierung
'86'	Refund:	Gutschrift:	Refund:	Gutschrift:
'87'	Cancellation	Abbruch	Cancellation	Abbruch
'88'	D/C Menu	D/C–Menü	D/C Menu	D/C–Menü
'89'	Precomp. Number	Vorautorisierungsnr.	Precomp. Number	Vorautoris.nr.
'8A'	Get Merchant PIN	Händler–PIN benötigt	Get Merchant PIN	Händl–PIN benö.

Table 1-15.16 - Messages for Display (German) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	German	English	German
'8B'	Data required in the DB	Daten notw. in DB	Need data in DB	
'8C'	Interval (MM)	Intervall (mm)	Interval (MM)	Intervall (mm)
'8D'	Number Attempts	Anzahl Versuche	Number Attempts	Anzahl Versuche
'8E'	Load Stop List	Lade Sperrliste	Load Stop List	Lade Sperrliste
'8F'	Pick up Card	Karte entnehmen	Pick up Card	Karte entnehmen
'90'	Denied:	Abgelehnt:	Denied:	Abgelehnt:
'91'	View Balance?	Zeige Guthaben?	View Balance?	Zeige Guthaben?
'92'	Do not honor	Abgelehnt	Do not honor	Abgelehnt
'93'	Expired Card	Karte verfallen	Expired Card	Karte verfallen
'94'	Suspected fraud	Verdacht auf Betrug	Suspected fraud	Verd. auf Betrug
'95'	PIN exceeded	PIN zu oft falsch	PIN exceeded	PIN zu oft fal.
'96'	Refer Issuer	Bitte Bank kontakt	Refer Issuer	Bank kontaktier.
'97'	No card number	Keine Kartenummer	No card number	Keine Kartenum.
'98'	Excessive Amount	Betrag zu hoch	Excessive Amount	Betrag zu hoch
'99'	Counterfeit Card	Gefälschten Karten	Counterfeit Card	Gefälsch. Karten
'9A'	Format Error	Formatfehler	Format Error	Formatfehler
'9B'	Card issuer or	Kartenausgeber oder	Card issuer or	Kartenausgeber
'9C'	Switch inop.	Vorgang nicht mögl.	Switch inop.	Vorg. nicht mögl
'9D'	Bad Routing	Routingfehler	Bad Routing	Routingfehler
'9E'	Sys malfunction	Systemstörung	Sys malfunction	Systemstörung
'9F'	Yes	Ja	Yes	Ja
'A0'	No	Nein	No	Nein
'A1'	Capture Card	Karte einbehalten	Capture Card	Karte einbehalt.
'A2'	Money not taken	Trans. nicht gebucht	Money not taken	Trans.nicht geb.
'A3'	Exp. date (YYMM)	Ablaufdatum (JJMM)	Exp. date (YYMM)	Ablaufdat.(JJMM)
'A4'	Enter PAN	Eingabe PAN	Enter PAN	Eingabe PAN
'A5'	Enter Term ID	Eingabe Terminal-ID:	Enter Term ID	Eingabe T-ID:
'A6'	Params Required	Parameter benötigt	Params Required	Param. benötigt
'A7'	Forced online	Online gefordert	Forced online	Online gefordert
'A8'	Sale:	Zahlung:	Sale:	Zahlung:
'A9'	Refund:	Gutschrift:	Refund:	Gutschrift:
'AA'	Purse empty	Börse leer	Purse empty	Börse leer
'AB'	Set currency	Währung einstellen	Set currency	Währung\ einstellen
'AC'	Currency changed	Währung geändert	Currency changed	Währung geändert
'AD'	Terminal ID	Terminal ID	Terminal ID	Terminal ID
'AE'	Exceeds limit	Limit überschritten	Exceeds limit	Limit überschrit
'AF'	Invalid currency	Währung abgelehnt	Invalid currency	Währung abgeleh.

Table 1-15.16 - Messages for Display (German) (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	German	English	German
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	In Betrieb	Terminal ready	In Betrieb
'E1' 1)	No receipt	Kein Beleg	No receipt	Kein Beleg
'E2'				
'E3'	Error reading card	Kartenlesefehler	Card read error	Kartenlesefehler
'E4'	Card validated	Karte geprüft	Card validated	Karte geprüft
'E5'	Receipt wanted?	Beleg?	Receipt wanted?	Beleg?
'E6'	Printing receipt	Beleg wird gedruckt	Printing receipt	Beleg w.gedruckt
'E7'	Purchase interrupted	Kauf abgebrochen	Purchase stopped	Kauf abgebrochen
'E8'	Terminal failure	Terminalfehler	Terminal failure	Terminalfehler
'E9'	Terminal busy	Terminal im Vorgang	Terminal busy	Term. im Vorgang
'EA'	Out of order	Ausser Betrieb	Out of order	Ausser Betrieb
'EB'	Push	Bitte drücken	Push	Bitte drücken
'EC'	Enter PIN and Accept	Bitte PIN eingeben	Enter PIN/Accept	Bitte PIN eing.
'ED'	Swipe card	Karte durchziehen	Swipe card	Karte durchzieh.
'EE'	Insert card again	Karte wieder einf.	Insert card	Karte neu einf.
'EF'	PIN:	PIN:	PIN:	PIN:
'F0'	Buy:	Zahlung:	Buy:	Zahlung:
'F1'	Accept?	Bitte bestätigen	Accept?	Bitte bestätigen
'F2'	Bonus added	Bonus gebucht	Bonus added	Bonus gebucht
'F3'	Technical failure	Technisches Versagen	Tech. failure	Technisch. Vers.
'F4'	Try again later	Später versuchen	Try again later	Später versuchen
'F5'	Limit reached	Limit erreicht	Limit reached	Limit erreicht
'F6'	Card is blocked	Karte gesperrt	Card is blocked	Karte gesperrt
'F7'	Refer Acquirer	Acquirer kontakten	Refer Acquirer	Acquirer kontak.
'F8'	(X) PIN tries left	Noch (x) PIN-Versuch	(X) PIN tries left	Noch(x) PIN-Vers
'F9'	Invalid merchant	Händler unbekannt	Invalid merchant	Händl. unbekannt
'FA'	Card unknown	Karte unbekannt	Card unknown	Karte unbekannt
'FB'	Split payment?	Zahlung splitten?	Split payment?	Zahlung split?
'FC'	Card/amount recorded	Betrag gebucht	Data recorded	Betrag gebucht
'FD'	Identical purchase	Identische Zahlung	Identical trans.	Identische Zahl.
'FE'	(Action Code)	(Action Code)	(Action Code)	(Action Code)
'FF'	Invalid transaction	Ungültigt Transakt.	Invalid trans.	Ungültigt Trans.

Legend: 1) The message may flash on the display to attract the cardholder's attention.
2) A "–" or a "+" may be used instead of the "/".

Generally, when "(and)" are used, the actual value of whatever is inside the brackets is indicated.
(X) indicates actual value.

Message Codes 'EC' and 'F1' are proposed text

Some of the text messages in German are verbose and need being displayed using more than one line in the display. In the table above, the character "\n" designates a new line. The character shall not be printed.

1-15.6.3 Receipt Texts

1-15.6.3.1 A Below is table 1-15.17 that defines the regional German texts that shall be used when printing receipts.

Table 1-15.17 - Messages for Printing (German)

Receipt Line	Element	English	German
'MI4'	Phone	Phone:	Telefon:
'MI5'	Business Reg. number	Bus.Reg.No:	Ust ID:
'HI2'	Copy indicator	Copy	Kopie
'HI4a'	Prelim/post indicator	Preliminary	Vorläufig
'HI4b'	Prelim/post indicator	Post registration	<blank>
'HI4c'	Cancellation indicator	Cancellation	Storno
'HI5'	Non-financial indicator	This is not a receipt	Nicht eine Beleg
'HI7a'	Transaction indicator	Authorization only	Autorisierung
'HI7b'		Refund	Gutschrift
'HI7c'		Reversal (auth)	Storno-Autorisierung
'HI7d'		<as in transaction>	<as in transaction>
'HI7e'		Cash	Bargeldauszahlung
'AM2a'	Amount type	Purchase	Bezahlung
'AM2b'		Refund	Gutschrift
'AM2c'		Cash	Bargeld
'AM2d'		Amount	Betrag
'AM4'	V.A.T.	VAT incl.	MwSt ent.
'AM5'	Surcharge	Surcharge	Zuslag
'AM6'	Cashback	Cashback	Cashback
'AM7' / 'AM11'	Extra	Extra	Trinkgeld
'AM9' / 'AM13'	Total	Total	Gesamtsum.
'TR1'	PIN indicator	PIN used	<blank>
'TR3'	Payment code	Paym.code:	<not applicable>
'TR4a'	Account type	Saving transaction	<not applicable>
'TR4b'		Debit transaction	<not applicable>
'TR4c'		Credit transaction	<not applicable>
'TR8'	Merchant number	Me.No:	VU-nr:
'TR12'	Status	Status:	Status:
'TR13'	Auth.code	Auth.code:	Genehmigungs Nr:
'TR14'	Auth.result	Authorized	Autorisiert
'SI2/SI4'	Tips info – 1	** When tipping **	** Bei Tipps **
'SI3/SI5'	Tips info –2	Ask for new receipt	Neues beleg anfordern
'SI6/SI7'a	Approval message	Approved for \ crediting of account	<not applicable>
'SI6/SI7'b		Approved for debiting\ of account as above	<not applicable>
'SI8'	Card reference	Printed digits:	Gedr. ziffern:

Table 1-15.17 - Messages for Printing (German) (*concluded*)

Receipt Line	Element	English	German
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	Legitimation:\ (ID-karten usw.)
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	Zuständigk. der Ausstell
'SI16'	ID expiry date	ID expiry date:	ID Ablaufdatum
'SI18'	Clerk ID	Clerk ID:	Händler ID:
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholders account by the issuer	<blank>
'SI26'a	Signatory type	Merchant's signature	Unterschrift Händler
'SI26'b		Cardholders signature	Unterschrift
'FI2'a	Termination reason	Interrupted – cancel	Vorgang Abgebrochen
'FI2'b		Declined	Vorgang Abgelehnt
'FI2'c		Signature declined	Unterschrift – Abgelehnt
'FI2'd		Interrupted – error	Vorgang Abgebrochen
'FI7'		Retain receipt	Bitte beleg aufbewahren
'FI8'a	Recipient indicator	Cardholders' receipt	Kundenbeleg
'FI8'b		Merchant's receipt	Händler beleg
'PC3'	Balance amount	Balance	Saldo
'PC4'	Expiry date	Exp.date	Verfalldatum

1-15.7 Poland

1-15.7.1 Functional Requirements

Additional requirements

NOTE: In Poland, a fiscal printer shall be used for the sales system. The requirements for such printer are out of scope for this specification.

- 1-15.7.1.1 B The terminal shall support the language specific characters required for displaying and printing the Polish texts.

1-15.7.2 Display Texts

- 1-15.7.2.1 A Below is table 1-15.18 that defines the regional texts that shall be used when displaying text where Polish is the language chosen.

Table 1-15.18 - Messages for Display (Polish)

Message Code	20 Characters Display		16 Characters Display	
	English	Polish	English	Polish
'01'	(Amount)	(Kwota)	(Amount)	(Kwota)
'02'	(Amount) OK?	Akceptuj (Kwota)	(Amount) OK?	Akcept. (Kwota)
'03'	Approved	Autoryzacja OK	Approved	Autoryzacja OK
'04'	Call Your Bank	Zadzwoń do banku	Call Your Bank	Zadzwoń do banku
'05'	Cancel or Enter	Anuluj/Akceptuj	Cancel or Enter	Anuluj/Akceptuj
'06'	Card Error	Błąd karty	Card Error	Błąd karty
'07'	Declined	Operacja odrzucona	Declined	Operacja odrzuc.
'08'	Enter Amount	Wprowadź kwotę	Enter Amount	Wprowadź kwotę
'09'	Enter PIN	Podaj kod PIN	Enter PIN	Podaj kod PIN
'0A'	Incorrect PIN	PIN	Incorrect PIN	Zły kod PIN
'0B'	Insert Card	Wczytaj kartę	Insert Card	Wczytaj kartę
'0C'	Not Accepted	Karta odrzucona	Not Accepted	Karta odrzucona
'0D'	PIN OK	Kod PIN zgodny	PIN OK	Kod PIN zgodny
'0E'	Please Wait	Proszę czekać...	Please Wait	Proszę czekać...
'0F'	Processing Error	Błąd techniczny	Processing Error	Błąd techniczny
'10'	Remove Card	Wyjmij kartę	Remove Card	Wyjmij kartę
'11'	Use Chip Reader	Użyj karty chipowej	Use Chip Reader	Użyj karty chip.
'12'	Use MAG Stripe	Użyj karty magnet.	Use MAG Stripe	Użyj karty magn.
'13'	Try Again	Spróbuj ponownie	Try Again	Spróbuj ponownie
'14'	Welcome		Welcome	
'15'	Present Card		Present Card	
'16'	Processing		Processing	
'17'	Card read OK. Please remove card		Card read OK. Remove card	
'18'	Please insert or swipe card		Please insert or swipe card	
'19'	Please present one card only		Please present one card only	
'1A' – '3F'	RFU for assignment by EMV			
'40'	System Error, retry	Błąd, próbuj ponownie	System Error	Błąd, powtórz
'41'	Invalid Card	Niewłaściwa karta	Invalid Card	Zła karta
'42'	Card out-of-order	Błąd na karcie	Error in card	Błąd na karcie
'43'	Expired Card	Karta już nieważna	Expired Card	Karta nieważna
'44'	Insufficient value	Za mała wartość	Too low value	Za mała wartość

Table 1-15.18 - Messages for Display (Polish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Polish	English	Polish
'45'	Card not present	Brak karty	Card missing	Brak karty
'46'	Data Store full	Pamięć zapełniona	Data Store full	Pamięć pełna
'47'	Timed out	Przekroczony czas	Timed out	Przekr. czas
'48'	Thank You	Dziękuję	Thank You	Dziękuję
'49'	Not available	Funkcja niedostępna	Not available	Funkcja niedost.
'4A'	Print receipt?	Drukować paragon?	Print receipt?	Wydruk paragonu?
'4B'	Cancel	Anuluj	Cancel	Anuluj
'4C'	Make Selection	Wybierz	Make Selection	Wybierz
'4D'	Incorrect Amount	Błędna kwota	Wrong Amount	Błędna kwota
'4E'	Welcome	Witamy	Welcome	Witamy
'4F'	Signature	Podpis	Signature	Podpis
'50'	Application Menu	Menu aplikacji	Menu	Menu aplikacji
'51'	Transaction Menu	Manu transakcji	Menu	Manu transakcji
'52'	Purchase	Zakup	Purchase	Zakup
'53'	Page	Strona	Page	Strona
'54'	PIN Blocked	Kod PIN zablokowany	PIN Blocked	PIN zablokowany
'55'	Enter New PIN	Wprowadź nowy PIN	Enter New PIN	Podaj nowy PIN
'56'	PIN Changed	Kod PIN zmieniony	PIN Changed	PIN zmieniony
'57'	PIN Unchanged	PIN nie zmieniony	PIN Unchanged	PIN nie zmien.
'58'	2 PINs not same	2 różne kody PIN	2 PINs not same	2 różne kody PIN
'59'	Confirm new PIN	Potwierdź nowy PIN	Confirm new PIN	Potw. nowy PIN
'5A'	Change PIN	Zmień kod PIN	Change PIN	Zmień kod PIN
'5B'	Unblock PIN	Odblokuj kod PIN	Unblock PIN	Odblokuj kod PIN
'5C'	PIN not blocked	PIN nie zablokowany	PIN not blocked	PIN nie zablok.
'5D'	PIN Unblocked	PIN odblokowany	PIN Unblocked	PIN odblokowany
'5E'	Calling...	Wybieram numer...	Calling...	Wybieram numer...
'5F'	Transmitting...	Transmisja...	Transmitting...	Transmisja...
'60'	Receiving...	Odbieranie...	Receiving...	Odbieranie...
'61'	Comms Error	Błąd komunikacji	Comms Error	Błąd komunikacji
'62'	Disconnecting	Rozłączenie	Disconnecting	Rozłączenie
'63'	Trans Log Upload	Przesyłam log trans.	Trans Log Upload	Wysyłam log tr.
'64'	Retrying	Próbuję ponownie	Retrying	Próbuję ponownie
'65'	Upload Done	Wysłanie OK	Upload Done	Wysłanie OK

Table 1-15.18 - Messages for Display (Polish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Polish	English	Polish
'66'	Upload Failed	Błąd przy wysyłaniu	Upload Failed	Błąd wysyłania
'67'	No Records	Brak danych	No Records	Brak danych
'68'	Debit:	Obciążenie:	Debit:	Obciążenie:
'69'	Credit:	Uznanie:	Credit:	Uznanie:
'6A'	Credit Reversal	Zwrot uznania	Credit Reversal	Zwrot uznania
'6B'	Cash Load	Ładowanie karty	Cash Load	Ładowanie karty
'6C'	Balance:	Saldo:	Balance:	Saldo:
'6D'	New Balance	Nowe saldo	New Balance	Nowe saldo
'6E'	Specify Amount	Podaj kwotę	Specify Amount	Podaj kwotę
'6F'	Recovery Needed	Odtwórz system	Recovery Needed	Odtwórz system
'70'	Insufficient Funds	Za wysoka kwota	Value too high	Za wysoka kwota
'71'	Recovery Failed	Błąd odtworzenia	Recovery Failed	Błąd odtworzenia
'72'	Recovery Done	Odtworzenie OK	Recovery Done	Odtworzenie OK
'73'	Money Taken	Pobrano kwotę	Money Taken	Pobrano kwotę
'74'	Show Balance	Pokaż saldo	Show Balance	Pokaż saldo
'75'	Statement Review	Pokaż wyciąg	Statement Review	Pokaż wyciąg
'76'	by issuer	w/g wydawcy	by issuer	w/g wydawcy
'77'	Upload Time	Czas wysyłki	Upload Time	Czas wysyłki
'78'	Start (HH:MM)	Start (tt:mm)	Start (HH:MM)	Start (tt:mm)
'79'	End (HH:MM)	Koniec (tt:mm)	End (HH:MM)	Koniec (tt:mm)
'7A'	Prefix No	Prefiks	Prefix No	Prefiks
'7B'	Totals	Sumy	Totals	Sumy
'7C'	Auth X25 No	Autoryzacja X.25 nr	Auth X25 No	Autoryz. X.25 nr
'7D'	Upload X25 No	Wysyłka X.25 nr	Upload X25 No	Wysyłka X.25 nr
'7E'	No Trials:	Liczba prób:	No Trials:	Liczba prób:
'7F'	Delay:	Opóźnienie:	Delay:	Opóźnienie:
'80'	Onl Auth. Data	Dane autoryz. online	Onl Auth. Data	Dane aut. online
'81'	Onl Upload Data	Dane wsadowe online	Onl Upload Data	Dane wsad. onl.
'82'	Get Cash	Pobranie gotówki	Get Cash	Pobranie gotówki
'83'	Unblock Appli.	Odblokuj aplikację	Unblock Appli.	Odbl. aplikację
'84'	Pre-Autho.	Preautoryzacja	Pre-Autho.	Preautoryzacja
'85'	Pre Completion	Dopełnienie preaut.	Pre Completion	Dopełn. preaut.
'86'	Refund:	Zwrot:	Refund:	Zwrot:

Table 1-15.18 - Messages for Display (Polish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Polish	English	Polish
'87'	Cancellation	Anulowanie	Cancellation	Anulowanie
'88'	D/C Menu	Menu obciążenie/uzn.	D/C Menu	Menu obc./uzn.
'89'	Precomp. Number	Nr preautoryzacji	Precomp. Number	Nr preautoryz.
'8A'	Get Merchant PIN	Pobierz PIN	Get Merchant PIN	Pobierz PIN
'8B'	Data required in the DB	Wymagane dane bazy	Need data in DB	Wym. dane bazy
'8C'	Interval (MM)	Przedział czasu (mm)	Interval (MM)	Czas (mm)
'8D'	Number Attempts	Liczba prób	Number Attempts	Liczba prób
'8E'	Load Stop List	Załaduj stoplistę	Load Stop List	ładuj stoplistę
'8F'	Pick up Card	Zatrzymaj kartę	Pick up Card	Zatrzymaj kartę
'90'	Denied:	Odrzucone:	Denied:	Odrzucone:
'91'	View Balance?	Pokazać saldo?	View Balance?	Pokazać saldo?
'92'	Do not honor	Karta nie uznawana	Do not honor	Karta nie uznaw.
'93'	Expired Card	Ważność wygasła	Expired Card	Ważność wygasła
'94'	Suspected fraud	Możliwe oszustwo	Suspected fraud	Możliwe oszustwo
'95'	PIN exceeded	Za dużo prób PINu	PIN exceeded	Za dużo prób PIN
'96'	Refer Issuer	Zadzwoń do wydawcy	Refer Issuer	Dzwoń do wydawcy
'97'	No card number	Brak numeru karty	No card number	Brak nr karty
'98'	Excessive Amount	Zbyt wysoka kwota	Excessive Amount	Za wysoka kwota
'99'	Counterfeit Card	Fałszywa karta	Counterfeit Card	Fałszywa karta
'9A'	Format Error	Błąd formatu	Format Error	Błąd formatu
'9B'	Card issuer or	Wydawca lub	Card issuer or	Wydawca lub
'9C'	Switch inop.	Switch nie odpowiada	Switch inop.	Switch nie odp.
'9D'	Bad Routing	Błąd routingu	Bad Routing	Błąd routingu
'9E'	Sys malfunction	Błąd systemu	Sys malfunction	Błąd systemu
'9F'	Yes	Tak	Yes	Tak
'A0'	No	Nie	No	Nie
'A1'	Capture Card	Zatrzymaj kartę	Capture Card	Zatrzymaj kartę
'A2'	Money not taken	Kwota nie pobrana	Money not taken	Kwota nie pobr.
'A3'	Exp. date (YYMM)	Data ważności (RRMM)	Exp. date (YYMM)	Data ważn. (RRMM)
'A4'	Enter PAN	Podaj numer karty	Enter PAN	Podaj nr karty
'A5'	Enter Term ID	Podaj ID terminala	Enter Term ID	Podaj ID terminala
'A6'	Params Required	Wymagane parametry	Params Required	Wymagane param.

Table 1-15.18 - Messages for Display (Polish) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Polish	English	Polish
'A7'	Forced online	Wymuszenie on-line	Forced online	Wymuś on-line
'A8'	Sale:	Sprzedaż:	Sale:	Sprzedaż:
'A9'	Refund:	Zwrot zapłaty:	Refund:	Zwrot zapłaty:
'AA'	Purse empty	Portfel jest pusty	Purse empty	Portfel pusty
'AB'	Set currency	Ustaw walutę	Set currency	Ustaw walutę
'AC'	Currency changed	Zmieniono walutę	Currency changed	Zmieniono walutę
'AD'	Terminal ID	ID terminala	Terminal ID	ID terminala
'AE'	Exceeds limit	Przekroczony limit	Exceeds limit	Przekr. limit
'AF'	Invalid currency	Niewłaściwa waluta	Invalid currency	Błędna waluta
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	Terminal gotowy	Terminal ready	Terminal gotowy
'E1' 1)	No receipt	Bez potwierdzenia	No receipt	Bez potwierdz.
'E2'				
'E3'	Error reading card	Błąd odczytu karty	Card read error	Błąd odczytu
'E4'	Card validated	Karta potwierdzona	Card validated	Karta potw.
'E5'	Receipt wanted?	Wydruk paragonu?	Receipt wanted?	Wydruk paragonu?
'E6'	Printing receipt	Drukowanie paragonu	Printing receipt	Drukowanie par.
'E7'	Purchase interrupted	Zakup przerwany	Purchase stopped	Zakup przerwany
'E8'	Terminal failure	Błąd terminala	Terminal failure	Błąd terminala
'E9'	Terminal busy	Terminal zajęty	Terminal busy	Terminal zajęty
'EA'	Out of order	Nieczynny	Out of order	Nieczynny
'EB'	Push	Naciśnij	Push	Naciśnij
'EC'	Enter PIN and Accept	Podaj PIN / Akceptuj	Enter PIN/Accept	Podaj PIN/Akc.
'ED'	Swipe card	Wczytaj kartę	Swipe card	Wczytaj kartę
'EE'	Insert card again	Wczytaj ponownie	Insert card	Wczytaj ponownie
'EF'	PIN:	PIN:	PIN:	PIN:
'F0'	Buy:	Zakup:	Buy:	Zakup:
'F1'	Accept?	Naciśnij Akceptuj	Accept?	Naciśnij Akcept.
'F2'	Bonus added	Dodano bonus	Bonus added	Dodano bonus
'F3'	Technical failure	Błąd techniczny	Tech. failure	Błąd techniczny
'F4'	Try again later	Spróbój później	Try again later	Spróbój później
'F5'	Limit reached	Osiągnięty limit	Limit reached	Osiągnięty limit
'F6'	Card is blocked	Karta zablokowana	Card is blocked	Karta zablok.

Table 1-15.18 - Messages for Display (Polish) (concluded)

Message Code	20 Characters Display		16 Characters Display	
	English	Polish	English	Polish
'F7'	Refer Acquirer	Zadzwoń do centrum	Refer Acquirer	Dzwoń do centrum
'F8'	(X) PIN tries left	Zostało (X) prób PIN	(X) PIN tries left	Zostało (X) prób
'F9'	Invalid merchant	Nieznany akceptant	Invalid merchant	Nieznany akcept.
'FA'	Card unknown	Nieznana karta	Card unknown	Nieznana karta
'FB'	Split payment?	Podział zapłaty?	Split payment?	Podział zapłaty?
'FC'	Card/amount recorded	Karta/kwota zapisane	Data recorded	Karta/kw. zapis.
'FD'	Identical purchase	Identyczny zakup	Identical trans.	Identyczny zakup
'FE'	(Action Code)	(Action Code)	(Action Code)	(Action Code)
'FF'	Invalid transaction	Niezgodna transakcja	Invalid trans.	Niezgodna trans.

Legend: ¹⁾ The message may flash on the display to attract the cardholder's attention.
²⁾ A "-" or a "+" may be used instead of the "/".
 Generally, when "(and)" are used, the actual value of whatever is inside the brackets is indicated.
 (X) indicates actual value.
 Message Codes 'EC' and 'F1' are proposed text

1-15.7.3 Receipt texts

To be defined

1-15.8 Iceland

1-15.8.1 Functional Requirements

Nets Denmark A/S is not aware of any specific Icelandic requirements not already specified either in this document or in the referenced documents.

1-15.8.2 Display Texts

- 1-15.8.2.1 B Regional texts that shall be used when displaying text where Icelandic is the language chosen are defined in table 1-15.19 below.

Table 1-15.19 - Messages for Display (Icelandic)

Message Code	20 Characters Display		16 Characters Display	
	English	Icelandic	English	Icelandic
'01'	(Amount)	(Amount)(Cur.Code)	(Amount)	(Amount)(Cur.Code)
'02'	(Amount) OK?	(Amnt)(Cur.Code) Í lagi?	(Amount) OK?	(Amnt)(Cur.Code) Í lagi?
'03'	Approved	Heimilað	Approved	Heimilað
'04'	Call Your Bank	Samband við banka	Call Your Bank	Samb. við banka
'05'	Cancel or Enter	Hætta eða Staðfesta	Cancel or Enter	Hætta/Staðfesta
'06'	Card Error	Villa í korti	Card Error	Villa í korti
'07'	Declined	Hafnað	Declined	Hafnað
'08'	Enter Amount	Sláið inn upphæð	Enter Amount	Sláið inn upphæð
'09'	Enter PIN	Sláið inn PIN	Enter PIN	Sláið inn PIN
'0A'	Incorrect PIN	Rangt PIN númer	Incorrect PIN	Rangt PIN númer
'0B'	Insert Card	Settu kortið í	Insert Card	Settu kortið í
'0C'	Not Accepted	Ekki heimilað	Not Accepted	Ekki heimilað
'0D'	PIN OK	PIN í lagi	PIN OK	PIN í lagi
'0E'	Please Wait	Augnablik	Please Wait	Augnablik
'0F'	Processing Error	Kerfisvilla	Processing Error	Kerfisvilla
'10'	Remove Card	Fjarlægjið kortið	Remove Card	Fjarlægjið kortið
'11'	Use Chip Reader	Notið örgjörvaesara	Use Chip Reader	Notið örgjörvann
'12'	Use MAG Stripe	Notið segulröndina	Use MAG Stripe	Notið segulrönd
'13'	Try Again	Reynið aftur	Try Again	Reynið aftur
'14'	Welcome	Velkomin(n)	Welcome	Velkomin(n)
'15'	Present Card	Afhenta/Sýna kort	Present Card	Sýna kort
'16'	Processing	Í vinnslu	Processing	Í vinnslu
'17'	Card read OK. Please remove card	Kortið er lesið Fjarlægjið kortið	Card read OK. Remove card	Kortið er lesið Fjarlægjið kortið
'18'	Please insert or swipe card	Settu kort í/Rennið	Please insert or swipe card	Settu í/Rennið
'19'	Please present one card only	Aðeins eitt kort	Please present one card only	Aðeins eitt kort
'1A' – '3F'	RFU for assignment by EMV			

Table 1-15.19 - Messages for Display (Icelandic) (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Icelandic	English	Icelandic
'40'	System Error, retry	Kerfisvilla/Re.aftur	System Error	Kerfisvilla
'41'	Invalid Card	Ógilt kort	Invalid Card	Ógilt kort
'42'	Card out–of–order	Kort ónothæft	Error in card	Kort ónothæft
'43'	Expired Card	Útrunnið kort	Expired Card	Útrunnið kort
'44'	Insufficient value	Ekki næg innistæða	Too low value	Innistæða of lág
'45'	Card not present	Kort ekki til staðar	Card missing	Kort ekki víst
'46'	Data Store full	Gagnageymsla full	Data Store full	Gagnageym.full
'47'	Timed out	Tími útrunninn	Timed out	Tími útrunninn
'48'	Thank You	Takk fyrir	Thank You	Takk fyrir
'49'	Not available	Ekki mögulegt	Not available	Ekki mögulegt
'4A'	Print receipt?	Prenta kvittun?	Print receipt?	Prenta kvittun?
'4B'	Cancel	Hætta	Cancel	Hætta
'4C'	Make Selection	Veldu	Make Selection	Veldu
'4D'	Incorrect Amount	Röng upphæð	Wrong Amount	Röng upphæð
'4E'	Welcome	Velkomin(n)	Welcome	Velkomin(n)
'4F'	Signature	Undirskrift	Signature	Undirskrift
'50'	Application Menu	Valmynd	Menu	Valmynd
'51'	Transaction Menu	Valmynd	Menu	Valmynd
'52'	Purchase	Viðskipti	Purchase	Viðskipti
'53'	Page	Síða	Page	Síða
'54'	PIN Blocked	PIN læstur	PIN Blocked	PIN læstur
'55'	Enter New PIN	Sláðu inn nýtt PIN	Enter New PIN	Nýtt PIN
'56'	PIN Changed	PIN er breytt	PIN Changed	PIN er breytt
'57'	PIN Unchanged	PIN er óbreytt	PIN Unchanged	PIN er óbreytt
'58'	2 PINs not same	2 PIN eru ekki eins	2 PINs not same	2 PIN ekki eins
'59'	Confirm new PIN	Staðfesta nýtt PIN	Confirm new PIN	Staðfesta PIN
'5A'	Change PIN	Breyta PIN	Change PIN	Breyta PIN
'5B'	Unblock PIN	Opna PIN	Unblock PIN	Opna PIN
'5C'	PIN not blocked	PIN ekki læst	PIN not blocked	PIN ekki læst
'5D'	PIN Unblocked	PIN aflæst	PIN Unblocked	PIN aflæst
'5E'	Calling...	Hringir...	Calling...	Hringir...
'5F'	Transmitting...	Sendir...	Transmitting...	Sendir...
'60'	Receiving...	Móttekur...	Receiving...	Móttekur...
'61'	Comms Error	Samskiptavilla	Comms Error	Samskiptavilla
'62'	Disconnecting	Aftengist	Disconnecting	Aftengist
'63'	Trans Log Upload	Færsluskrá upphal	Trans Log Upload	Færslu upphal
'64'	Retrying	Reyni aftur	Retrying	Reyni aftur
'65'	Upload Done	Upphal lokið	Upload Done	Upphal lokið

Table 1-15.19 - Messages for Display (Icelandic) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Icelandic	English	Icelandic
'66'	Upload Failed	Upphal mistókst	Upload Failed	Upphal mistókst
'67'	No Records	Engar færslur	No Records	Engar færslur
'68'	Debit:	Debet:	Debit:	Debet:
'69'	Credit:	Kredit:	Credit:	Kredit:
'6A'	Credit Reversal	Kredit bakfært:	Credit Reversal	Kredit bakfært:
'6B'	Cash Load	Reiðufé hleðsla:	Cash Load	Fé hleðsla:
'6C'	Balance:	Staða:	Balance:	Staða:
'6D'	New Balance	Ný staða:	New Balance	Ný staða:
'6E'	Specify Amount	Sláið inn upphæð	Specify Amount	Sláið inn upphæð
'6F'	Recovery Needed	Leiðréttá villu	Recovery Needed	Leiðréttá villu
'70'	Insufficient Funds	Ekki næg innistæða	Value too high	Ekki næg innist.
'71'	Recovery Failed	Villa ekki leiðrétt	Recovery Failed	Villa ekki leiðr
'72'	Recovery Done	Villa leiðrétt	Recovery Done	Villa leiðrétt
'73'	Money Taken	Upphæð dregin frá	Money Taken	Upphæð dregin
'74'	Show Balance	Sýna stöðu	Show Balance	Sýna stöðu
'75'	Statement Review	Sjá reikningsyfirlit	Statement Review	Reikningsyfirlit
'76'	by issuer	Af útgefanda	by issuer	Af útgefanda
'77'	Upload Time	Upphal tími	Upload Time	Upphal tími
'78'	Start (HH:MM)	Byrja (hh:mm)	Start (HH:MM)	Byrja (hh:mm)
'79'	End (HH:MM)	Enda (hh:mm)	End (HH:MM)	Enda (hh:mm)
'7A'	Prefix No	BIN Nr	Prefix No	BIN Nr
'7B'	Totals	Samtals	Totals	Samtals
'7C'	Auth X25 No	Heimild X25 Nr	Auth X25 No	Heimild X25 Nr
'7D'	Upload X25 No	Upphal X25 Nr	Upload X25 No	Upphal X25 Nr
'7E'	No Trials:	Fjöldi tilrauna:	No Trials:	Fjöldi tilrauna:
'7F'	Delay:	Töf:	Delay:	Töf:
'80'	Onl Auth. Data	Heimildar gögn	Onl Auth. Data	Heimildar gögn
'81'	Onl Upload Data	Upphal gögn	Onl Upload Data	Upphal gögn
'82'	Get Cash	Reiðufé úttekt	Get Cash	Reiðufé úttekt
'83'	Unblock Appli.	Fjarl. Lás af appl.	Unblock Appli.	Lás af appl.
'84'	Pre–Autho.	Bráðabirgða heimild	Pre–Autho.	Bráðab. Heimild
'85'	Pre Completion	Bráðabirgða niðurst.	Pre Completion	Bráðab.Niðurst.
'86'	Refund:	Endurgreiðsla:	Refund:	Endurgreiðsla:
'87'	Cancellation	Ógilding	Cancellation	Ógilding
'88'	D/C Menu	Valmynd	D/C Menu	Valmynd
'89'	Precomp. Number	Fyrirfr.reiknað Nr	Precomp. Number	Fyrirfr.reik.Nr
'8A'	Get Merchant PIN	Söluaðila PIN	Get Merchant PIN	Söluaðila PIN

Table 1-15.19 - Messages for Display (Icelandic) (continued)

Message Code	20 Characters Display		16 Characters Display	
	English	Icelandic	English	Icelandic
'8B'	Data required in the DB	Gagna krafist úr G.G.	Need data in DB	Gögn krafín
'8C'	Interval (MM)	Tímabil(MM)	Interval (MM)	Tímabil(MM)
'8D'	Number Attempts	Fjöldi tilrauna	Number Attempts	Fjöldi tilrauna
'8E'	Load Stop List	Hlaða ógildingar skrá	Load Stop List	Hlaða ógild.skrá
'8F'	Pick up Card	Taka kort	Pick up Card	Taka kort
'90'	Denied:	Hafnað:	Denied:	Hafnað:
'91'	View Balance?	Sýna stöðu?	View Balance?	Sýna stöðu?
'92'	Do not honor	Hafnað	Do not honor	Hafnað
'93'	Expired Card	Útrunnið kort	Expired Card	Útrunnið kort
'94'	Suspected fraud	Hugsanlegt svindl	Suspected fraud	Grunur um svindl
'95'	PIN exceeded	Of mörg röng PIN	PIN exceeded	Of mörg röng PIN
'96'	Refer Issuer	Samb. við útgefanda	Refer Issuer	Samb. útgefanda
'97'	No card number	Ekkert kortanúmer	No card number	Ekkert kort nr
'98'	Excessive Amount	Upphæð of há	Excessive Amount	Upphæð of há
'99'	Counterfeit Card	Falsað kort	Counterfeit Card	Falsað kort
'9A'	Format Error	Snið(format) villa	Format Error	Snið villa
'9B'	Card issuer or	Kort útgefandi eða	Card issuer or	Kort útgef. eða
'9C'	Switch inop.	Switch óvirkur	Switch inop.	Switch óvirkur
'9D'	Bad Routing	Gagnavegur rangur	Bad Routing	Gagnav.rangur
'9E'	Sys malfunction	Kerfisbilun	Sys malfunction	Kerfisbilun
'9F'	Yes	Já	Yes	Já
'A0'	No	Nei	No	Nei
'A1'	Capture Card	Taka kort	Capture Card	Taka kort
'A2'	Money not taken	Upphæð ekki gjaldf.	Money not taken	Upph.ekki gjaldf
'A3'	Exp. date (YYMM)	Gildistími(ÁÁMM)	Exp. date (YYMM)	Gildistími
'A4'	Enter PAN	Sláið inn kortanúmer	Enter PAN	Sláið inn kortNr
'A5'	Enter Term ID	Sláið inn Posa Id	Enter Term ID	Sláið inn Posald
'A6'	Params Required	Breytu krafist	Params Required	Breytu krafist
'A7'	Forced online	Sækja heimild	Forced online	Sækja heimild
'A8'	Sale:	Sala:	Sale:	Sala:
'A9'	Refund:	Endurgreiðsla:	Refund:	Endurgreiðsla:
'AA'	Purse empty	Kassinn er tómur	Purse empty	Kassinn er tómur
'AB'	Set currency	Tilgreinið gjaldm.	Set currency	Tilg. Gjaldm.
'AC'	Currency changed	Gjaldmiðli breytt	Currency changed	Gjaldmið.breytt
'AD'	Terminal ID	Posa Id:	Terminal ID	Posa Id:
'AE'	Exceeds limit	Hámarki náð	Exceeds limit	Hámarki náð
'AF'	Invalid currency	Ógildur gjaldmiðill	Invalid currency	Ógild mynt

Table 1-15.19 - Messages for Display (Icelandic) (concluded)

Message Code	20 Characters Display		16 Characters Display	
	English	Icelandic	English	Icelandic
'B0' – 'DF'	RFU for assignment by TAPA			
'E0'	Terminal ready	Posinn er klár	Terminal ready	Posinn er klár
'E1' 1)	No receipt	Engin kvittun	No receipt	Engin kvittun
'E2'				
'E3'	Error reading card	Villa við kortalestur	Card read error	Villa les. kort
'E4'	Card validated	Kort heimilað	Card validated	Kort heimilað
'E5'	Receipt wanted?	Prenta kvittun?	Receipt wanted?	Prenta kvittun?
'E6'	Printing receipt	Prentar kvittun	Printing receipt	Prentar kvittun
'E7'	Purchase interrupted	Hætt við viðskipti	Purchase stopped	Hætt við kaup
'E8'	Terminal failure	Posi bilaður	Terminal failure	Posi bilaður
'E9'	Terminal busy	Posi upptekinn	Terminal busy	Posi upptekinn
'EA'	Out of order	Virkar ekki	Out of order	Virkar ekki
'EB'	Push	Ýta	Push	Ýta
'EC'	Enter PIN and Accept	Slá inn PIN–Staðfesta	Enter PIN/Accept	PIN og Staðfesta
'ED'	Swipe card	Rennið kortinu	Swipe card	Rennið kortinu
'EE'	Insert card again	Settu kortið aftur í	Insert card	Settu kortið í
'EF'	PIN:	PIN:	PIN:	PIN:
'F0'	Buy:	Viðskipti:	Buy:	Viðskipti:
'F1'	Accept?	Heimila?	Accept?	Heimila?
'F2'	Bonus added	Bónusi bætt við	Bonus added	Bónusi bætt við
'F3'	Technical failure	Tæknileg villa	Tech. failure	Tæknileg villa
'F4'	Try again later	Prófa aftur seinna	Try again later	Prófa seinna
'F5'	Limit reached	Hámarki náð	Limit reached	Hámarki náð
'F6'	Card is blocked	Kortið er læst	Card is blocked	Kortið er læst
'F7'	Refer Acquirer	Hringið til færsluh	Refer Acquirer	Hrin.til færsluh
'F8'	(X) PIN tries left	(x) PIN tilraun. eftir	(X) PIN tries left	(x)PIN tilraun.
'F9'	Invalid merchant	Söluaðili óþekktur	Invalid merchant	Söluaðili óþekk.
'FA'	Card unknown	Korti hafnað	Card unknown	Korti hafnað
'FB'	Split payment?	Deila greiðslu?	Split payment?	Deila greiðslu?
'FC'	Card/amount recorded	Kort/upphæð skráð?	Data recorded	Kort/upph. skráð
'FD'	Identical purchase	Nákvæmlega eins kaup	Identical trans.	Eins kaup
'FE'	(Action Code)	(Action Code)	(Action Code)	
'FF'	Invalid transaction	Ógild færsla	Invalid trans.	Ógild færsla
Legend: 1) The message may flash on the display to attract the cardholder's attention. 2) A “–” or a “+” may be used instead of the “/”. Generally, when (“and”) are used, the actual value of whatever is inside the brackets is indicated. (X) indicates actual value. Message Codes 'EC' and 'F1' are proposed text				

1-15.8.3 Receipt Texts

1-15.8.3.1 A Below is table 1-15.20 that defines the regional Icelandic texts that shall be used when printing receipts.

Table 1-15.20 - Messages for Printing (Icelandic)

Receipt Line	Element	English	Icelandic
'MI4'	Phone	Phone:	Sími:
'MI5'	Business Reg. number	Bus.Reg.No:	KT:
'HI2'	Copy indicator	Copy	Afrit:
'HI4a'	Prelim/post indicator	Preliminary	Bráðabirgða
'HI4b'	Prelim/post indicator	Post registration	Bakfærsla
'HI4c'	Cancellation indicator	Cancellation	Ógilding
'HI5'	Non–financial indicator	This is not a receipt	Ekki kvittun
'HI7a'	Transaction indicator	Authorization only	Aðeins heimild
'HI7b'		Refund	Endurgreiðsla
'HI7c'		Reversal (auth)	Ógilding færslu
'HI7d'		<as in transaction>	<as in transaction>
'HI7e'		Cash	Reiðufé
'AM2a'	Amount type	Purchase	Viðskipti
'AM2b'		Refund	Endurgreiðsla
'AM2c'		Cash	Peningar
'AM2d'		Amount	Upphæð
'AM4'	V.A.T.	VAT incl.	VSK
'AM5'	Surcharge	Surcharge	Viðbótar gjald
'AM6'	Cashback	Cashback	Peningar tilbaka
'AM7' / 'AM11'	Extra	Extra	Auka
'AM9' / 'AM13'	Total	Total	Samtals
'TR1'	PIN indicator	PIN used	PIN notaður
'TR3'	Payment code	Paym.code:	<not applicable>
'TR4a'	Account type	Saving transaction	<not applicable>
'TR4b'		Debit transaction	<not applicable>
'TR4c'		Credit transaction	<not applicable>
'TR8'	Merchant number	Me.No:	Viðskipta Nr:
'TR12'	Status	Status:	
'TR13'	Auth.code	Auth.code:	Heimild Nr:
'TR14'	Auth.result	Authorized	Heimilað
'SI2/SI4'	Tips info – 1	** When tipping **	**Þegar þjófófé**
'SI3/SI5'	Tips info –2	Ask for new receipt	Ný kvittun
'SI6/SI7'a	Approval message	Approved for \ crediting of account	<not applicable>
'SI6/SI7'b		Approved for debiting\ of account as above	<not applicable>
'SI8'	Card reference	Printed digits:	Tölustafir á korti:

Table 1-15.20 - Messages for Printing (Icelandic) (*concluded*)

Receipt Line	Element	English	Icelandic
'SI9/SI10'	ID source	Identification: \ (Passport etc.)	Skilríki:
'SI13'	Jurisdiction of issue	Jurisdiction of issue:	Útgefið af:
'SI16'	ID expiry date	ID expiry date:	Gildistími skilríkis:
'SI18'	Clerk ID	Clerk ID:	Afgreiðslumanns Nr:
'SI19/SI22'	Cash fee info	A fee or setup charge may be added to the cardholders account by the issuer	
'SI26'a	Signatory type	Merchant's signature	Undirskrift söluaðila
'SI26'b		Cardholders signature	Undirskrift korthafa
'FI2'a	Termination reason	Interrupted – cancel	Rofin – Hætt við
'FI2'b		Declined	Hafnað
'FI2'c		Signature declined	Undirskrift hafnað
'FI2'd		Interrupted – error	Rofin – Villa
'FI7'		Retain receipt	Geymdu kvittun
'FI8'a	Recipient indicator	Cardholders' receipt	Eintak korthafa
'FI8'b		Merchant's receipt	Eintak söluaðila
'PC3'	Balance amount	Balance	Inneign
'PC4'	Expiry date	Exp.date	Gildir út

This page is intentionally left blank

Index, Book 1

Page references in **bold** type refer to either figures or tables.

A

A-requirements, Definition, 1-4-7
AAC, Abbreviations, 1-4-1
AAR, Abbreviations, 1-4-1
Accelerated PIN Entry, 1-10-47
 Best Practice, 1-9-8
 Prepaid MSC, 1-10-47
Account Type, 1-15-16, 1-15-20
Account Type Selection, 1-10-15,
 1-10-25
Acquirer, 1-6-3
Acquirer Name, 1-10-26
Addition of Surcharges and Fees, Best
 Practice, 1-9-13
Additional Authorization, DCC, 1-10-79
additional transaction data in Issuer In-
 formation Envelope, Sweden,
 1-15-20
Administrative Functions, 1-11-22
AID, 1-14-13
 Abbreviations, 1-4-1
 Selection Record, **1-14-7**, 1-14-7
 Selection Table, 1-14-5
Amount Information, Receipts, 1-12-10
APE, Abbreviations, 1-4-1
Application Initialization, 1-14-2
Application Label, 1-12-14, 1-14-14
Application Preferred Name, 1-14-14
Application Priority Indicator, 1-14-16
Application Selection, 1-14-15
 Best Practice, 1-9-4
 Description, 1-14-3
Application Selection Indicator, 1-14-7
Approval Code, 1-9-6
Approved/Successful Transactions, Previ-
 ous Transaction Status, 1-10-32
ARQC, Abbreviations, 1-4-1
ASI
 Abbreviations, 1-4-1
 AID Selection Table, 1-14-7

ASN.1, Abbreviations, 1-4-1
ASW1 ASW2, Abbreviations, 1-4-1
ATM, Abbreviations, 1-4-1
ATR, Abbreviations, 1-4-1
Attributes for APACS 60 Messages, Nota-
 tion, 1-4-6
Authorization, 1-12-10
 Terms, 1-4-4
Authorization Reversal, Functionalities,
 1-10-7
Automated fuel dispensers, Receipt,
 1-12-4
Automatic Advice Transfer if no Custom-
 ers being Serviced, Best Practice,
 1-9-15
Availability, Previous Transaction Status,
 1-10-31

B

B-requirements, Definition, 1-4-7
Balance inquiry, Prepaid MSC, 1-10-48
Bank Acept Exception Rule, 1-15-29
Bank Acept Exception Rules, 1-15-29
Basic commands, 1-8-1
Basic Regulations, Denmark, 1-15-4
Basic Transaction Flow, 1-8-1, **1-8-4**
Batch Number, 1-9-17, 1-9-18
Bellcore attack, 1-14-18
Best Practice, 1-9-1
Bibliography, 1-4-12
Binary, Notation, 1-4-5
Bit Numbering, Notation, 1-4-5
Bonus data, Issuer Information Envelope,
 1-15-20
Build date, 1-14-2
Business Call, Terms, 1-4-4
Business Call and related signatory text,
 1-12-21
Business Calls, 1-11-20, **1-12-15**,
 1-12-17, **1-12-22**, 1-15-7

Business Calls and related header text,
1-12-11

Business Calls and Service Functions
Translated, **1-11-21**

Business Calls and Terminal Environ-
ments, 1-14-1

Business Requirements, 1-5-3, 1-14-1
Local PIN, 1-14-25

C

C-requirements, Definition, 1-4-7

CA, Abbreviations, 1-4-1

CAD, Abbreviations, 1-4-1

CAM, Abbreviations, 1-4-1

Cancellation

Business Call, 1-11-21

DCC, 1-10-79

Functionalities, 1-10-7

Sweden, 1-15-15

Candidate List, 1-14-13, 1-14-14,
1-14-15

Best Practice, 1-9-4

Number of entries, 1-14-13

Capture

Business Call, 1-11-21

Functionalities, 1-10-6

Car Rental, 1-6-1

DCC, 1-10-80

Card Data Entry, 1-12-16

Card Data Protection, 1-7-2

Card Data Source, Best Practice, 1-9-3

Card inserted correctly?, Best Practice,
1-9-3

Card Issuer, 1-6-3

Card Name, 1-14-14

AID Selection Table, 1-14-7

Card Product EMV Entry Point Paramet-
ers, AID Selection Table, 1-14-7

Card Product Flow, AID Selection Table,
1-14-7

Card Product Functions, AID Selection
Table, 1-14-7

Card Product Type, AID Selection Table,
1-14-7

Card Reconciliation Counter ID, 1-9-17

Card Reconciliation Counter Name,
1-9-17

Card Reference Key, 1-10-62

Card Validation (Booking), DCC, 1-10-78

Cardholder, 1-6-2

Cardholder Activated Terminals, 1-6-1

Cardholder Display, Terms, 1-4-4

Cardholder Verification, 1-14-22

PIN Entry, 1-14-22

Signature, 1-14-22

Cardholder Verification Method, Best
Practice, 1-9-4

Cardholder Verification Methods, 1-6-4

Cash

Functionalities, 1-10-10

Limitations, 1-6-4

Cash Advance Terminals, 1-6-2

Cash register, Best Practice, 1-9-12

Cash/Quasi-cash Terminals, **1-6-4**
Best Practice, 1-6-4

Cashback, 1-9-22, 1-10-16, 1-10-25

Best Practice, 1-9-13

Services, 1-11-21

Token, 1-10-58

Cashback Amount, Best Practice, 1-9-13

CAT, 1-6-1

Abbreviations, 1-4-1

Receipt, 1-12-3

CDA, Abbreviations, 1-4-1

CDP, Abbreviations, 1-4-1

Centralized log, 1-7-1

centralized logging, 1-7-2

CEP, Abbreviations, 1-4-1

Certification, 1-5-6

Characters, Receipts, 1-12-3, 1-12-6

Check-In - Card not present, DCC,
1-10-79

Check-In - Card present, DCC, 1-10-78

Check-Out, DCC, 1-10-80

Choice of Business Call, Best Practice,
1-9-2

CLA, Abbreviations, 1-4-1

Clock Frequency, Best Practice, 1-9-9

Combined MSC and ICC Application Se-
lection, 1-14-14

Command keys, Definition, **1-15-7**

Communication Session, Terms, 1-4-4

Compiled DCC receipt information,
1-12-36

CRC, Abbreviations, 1-4-2

CURRC, 1-12-11

Currency, 1-10-28
Currency Code, 1-12-11
 Cashback, 1-9-13
Currency Exponent, 1-10-28
Customer Reference Number, 1-10-14
CV-2, Abbreviation, 1-4-2
CVM, 1-3-2, 1-12-16
 Abbreviations, 1-4-2
CVM Status, 1-12-17
CVR, Abbreviations, 1-4-2

D

Danish letters, Display, 1-15-8
Danish regional receipts requirements,
 1-15-6
Danish Regulations, 1-15-4
Dankort, 1-9-18
 Denmark, 1-15-5
 Terms, 1-4-4
 Website, 1-4-13
Dankort Accelerated PIN Entry, Prepaid
 MSC, 1-10-47
Dankort Handbook, Denmark, 1-15-4
DAPE, Abbreviations, 1-4-2
Data Store, Defective, 1-9-16
Data Store Handler, General Require-
 ments, 1-14-21
Data Transmission, Best Practice, 1-9-8,
 1-9-9
Date Reconciliation, 1-9-17
Date, local transaction, 1-9-17
DCC - Dynamic Currency Conversion,
 Functionalities, 1-10-81
DCC currency conversion formulas, DCC,
 1-10-90
DCC functional requirement, Receipts,
 1-12-5
DCC Receipt Layout, 1-12-25
DCC transaction flow, **1-10-84**
DCC transaction types, 1-10-95
DCC-Transaction-Information, Attach-
 ment T, 1-10-87
DDA, Abbreviations, 1-4-2
DES and Triple DES, Notation, 1-4-6
Differential Power Analysis, 1-14-18
Diners, 1-9-18

Discretionary Data, **1-14-4**, 1-14-10
Display flow, 1-11-7
Display Rules, 1-14-14
Display texts
 Norway, 1-15-32
 Sweden, 1-15-21
Document Overview, **1-5-2**
DOL, 1-4-2
DPA, 1-14-18
DS, Abbreviations, 1-4-2
Dual Communication Platforms and Dual
 IP-Addresses, Best Practice, 1-9-14
Duplicate Transaction Check (PSAM),
 Best Practice, 1-9-12
Duplicate Transaction Check by the
 PSAM, 1-10-28

E

Early Amount, 1-4-4
ECBS, Abbreviations, 1-4-2
ECR, Abbreviations, 1-4-2
EFT-POS, Abbreviations, 1-4-2
Electronically stored journals, 1-14-24
Emphasizing of text, Receipts, 1-12-6
EMV, Abbreviations, 1-4-2
EMV Checksum, 1-14-2
Error Situations, Prepaid MSC, 1-10-49
Examples of Receipts, 1-12-38
Exception Handling
 MAD-Handler, 1-14-16
 Router, 1-14-16
Extended Authorization
 Business Call, 1-11-21
 Functionalities, 1-10-3
Extended Issuer Envelope, 1-10-12
Extra, 1-11-21

F

Fallback, 1-14-15, 1-14-22
 Best Practice, 1-9-3
 Key Entered Transaction, 1-14-22
 Non-Debit/Credit, 1-14-22
 Single Unit Terminal, 1-13-6, 1-13-7
 Transaction Condition Code, 1-12-16
Floor limit, 1-6-2
Footer Information, Receipts, 1-12-21

Forced CVM, Best Practice, 1-9-5
 Forced Offline
 Best Practice, 1-9-6
 Single Unit Terminal, 1-13-8
 Fuel Dispensers, Introduction, 1-6-1

G

Generic layout, Receipts, 1-12-7
 Get Amount 3, 1-9-8
 Get Debit/Credit Properties Command,
 Previous Transaction Status, 1-10-29
 Grand Total, 1-9-19
 Gratuity, 1-6-1, 1-10-6
 Best Practice, 1-9-13
 DCC, 1-10-91
 Denmark, 1-15-5
 Services, 1-11-21
 Guaranteed Reservation, DCC, 1-10-78
 Guidelines for evaluating the transaction
 result, **1-12-23**

H

Header Information, Receipts, 1-12-9
 Hexadecimal, Notations, 1-4-6
 Host Data Transfer, Prepaid MSC,
 1-10-47
 Host Interface info, 1-14-2
 Hotel, 1-6-1

I

I/O Buffer Size, 1-9-9
 ICC Application Selection, Description,
 1-14-12
 ICC Contactless, Transaction Condition
 Codes, 1-12-16
 ICC technology and Fallback to Magnetic
 Stripe, Best Practice, 1-9-3
 ICCR, Abbreviations, 1-4-2
 Iceland, 1-15-62
 ICS, Abbreviations, 1-4-2
 Identification Keys, DCC, 1-10-61
 IDPSAMAPP, 1-14-5, 1-14-7
 IFD, Abbreviations, 1-4-2
 IFSF, Abbreviations, 1-4-2

IFSF Field 48, 1-10-15
 IFSF Field 62, 1-10-15
 IFSF Field 63, 1-10-15
 INS, Abbreviations, 1-4-2
 Integrated Circuit Cards, 1-14-3
 International Standards, Introduction,
 1-5-1
 IP-address, 1-14-2
 ISDN, 1-9-14
 ISO/IEC, Abbreviations, 1-4-2
 Issuer Information Envelope Data
 Denmark, 1-15-5
 Sweden, 1-15-19

K

KCV, Abbreviations, 1-4-2
 KEK, Abbreviation, 1-4-2
 Key Enter, 1-10-25

L

Language Preference, 1-15-3
 Language Selection, ICC, 1-15-3
 Languages, 1-14-21
 Late Amount, 1-4-4
 Late Amount Entry, 1-10-24
 Limitations, Previous Transaction Status,
 1-10-31
 Loading, Prepaid MSC, 1-10-48
 Loading offline, Prepaid MSC, 1-10-49
 Local PIN, 1-14-25
 Best practice, 1-9-26
 Local PIN Verification, Description,
 1-14-20
 Lock
 Physical, 1-14-23
 Technician, 1-14-23
 Log, 1-14-24
 Description, 1-14-24
 Log and Totals, Best Practice, 1-9-15
 Log information, 1-7-2
 LRC, Abbreviations, 1-4-2
 Luhn formula, 1-10-50

M

MAC, Abbreviations, 1-4-2

MAD, Abbreviations, 1-4-2

Magnetic Stripe Cards, 1-14-3

Mail order, Transaction Condition Codes, 1-12-16

MasterCard, 1-9-18

MCC, Abbreviations, 1-4-2

MENAME, 1-12-8

Merchant, 1-6-2

Merchant Application Handler, Terminal interface, 1-14-21

Merchant Application Log, Best Practice, 1-9-16

Merchant Category Code, 1-4-2

Merchant data, Issuer Information Envelope, 1-15-20

Merchant information, 1-12-8

Merchant Initiative, 1-9-6, 1-12-17
Best Practice, 1-9-5

Messages for Display
Denmark, **1-11-2**
Finland, **1-15-41**
Germany, **1-15-48**
Norway, **1-15-33**
Poland, **1-15-56**
Sweden, **1-15-21**

Messages for Display (Danish), 1-15-8

Messages for Printing, Norway, **1-15-37**,
1-15-38, **1-15-46**

Messages for printing (Danish), 1-15-13

Messages for printing (reference), 1-12-94

Miscellaneous data, 1-15-20

Mounting of the PIN Entry Device, 1-9-27

MSC, Abbreviations, 1-4-2

MSC Application Selection, Description, 1-14-11

MSC Selection Record, Description, **1-14-4**

MSC Selection Table, 1-14-3

MSCR, Abbreviations, 1-4-2

MSD, Abbreviations, 1-4-2

MSD Contactless, Transaction Condition Codes, 1-12-16

Multi-entry, Terms, 1-4-4

N

Nets PSAM, 1-4-4

Network Model, Debit/Credit, **1-6-4**

No CVM, 1-15-1, 1-15-5
Denmark, 1-15-5

Norwegian regional receipt requirement, 1-15-29

Notation, 1-4-5

Number of Entries, Previous Transaction Status, 1-10-32

O

On Device CVM / Consumer Device CVM, Transaction Condition Codes, 1-12-16

Operators, Notation, 1-4-6

Optimizing the Transaction Time, Best Practice, 1-9-8

Cancellation, 1-12-10

Original Authorization, 1-12-11, 1-12-21,
1-12-22, 1-12-24, 1-12-31
Business Call, 1-11-21
Functionalities, 1-10-2

OTRS Terminal, 1-4-4

Out of Paper, 1-14-17

P

PAN, 1-10-28, 1-14-3
Abbreviations, 1-4-2
Previous Transaction Status, 1-10-30,
1-10-32
Ranges, 1-14-11

Paper Low, 1-14-17

Parallel Processing, Best Practice, 1-9-8

Password, 1-14-21, 1-14-23

Paying, Prepaid MSC, 1-10-48

Paying offline, Prepaid MSC, 1-10-49

Payment Card Industry - Data Security Standard, 1-7-1

Payment Condition Code, 1-10-17

Payment Conditions, Issuer Information Envelope, 1-15-20

PCI, Abbreviations, 1-4-2

PCI - DSS, 1-7-1

PCT
Abbreviations, 1-4-2
Data Objects, 1-10-26

- PED, Abbreviations, 1-4-2
 - PED info, 1-14-2
 - Phone order, Transaction Condition Codes, 1-12-16
 - Physically Secure Device, Definition, 1-14-18
 - PIN, 1-11-18
 - Abbreviations, 1-4-2
 - Tries, 1-11-19
 - PIN Entry, 1-11-8
 - PIN Entry flow, 1-11-18
 - PIN Pad
 - Keyboard, 1-14-19
 - ID, 1-14-19
 - PK, Abbreviations, 1-4-2
 - PKI, Abbreviations, 1-4-2
 - Placement and Installation of terminal, Best Practice, 1-9-27
 - Placement of the terminal, 1-9-27
 - Point of Service, Terms, 1-4-4
 - POS, Abbreviations, 1-4-2
 - POS Entry Mode, 1-12-16
 - Token, 1-10-57
 - POS Terminal/CAT Levels vs. Terminal Type, Best Practice, 1-6-5
 - Post Purchase, 1-11-21
 - Post Refund, 1-11-21
 - PP, Abbreviations, 1-4-2
 - PPK, Abbreviation, 1-4-2
 - PPS, Abbreviations, 1-4-2
 - PPSE, Abbreviations, 1-4-2
 - Pre-Receipt, DCC, 1-10-93
 - Preferred Offline, 1-10-21
 - Prepaid Card Information, Receipts, 1-12-24
 - Prepaid ICC Transactions, Functionalities, 1-10-33
 - Prepaid MSC Transaction Flow, 1-10-48
 - Prepaid MSC Transactions, Functionalities, 1-10-46
 - Primary Account Number, 1-14-3
 - Prepaid MSC, **1-10-50**
 - Private Label Card, Terms, 1-4-4
 - Private Label Card Scheme Recognition, 1-10-11
 - Processing Condition Table
 - Functionality, 1-10-22
 - Sweden, 1-15-15
 - Protected Functions, 1-14-23
 - Manufacturer Specific Functions, 1-14-23
 - PSAM, Abbreviations, 1-4-2
 - PSAM Code Checksum, 1-14-2
 - PSAM Config Checksum, 1-14-2
 - PSAM ID, 1-14-2
 - PSAM Subversion, 1-14-2
 - PSAM version no., 1-14-2
 - PSTN, 1-9-14
 - Cash, 1-12-10
 - Purchase, 1-10-2, 1-12-10, 1-12-11
 - Business Call, 1-11-21
- ## Q
- Quasi-Cash, Limitations, 1-6-5
 - qVSDC, Abbreviations, 1-4-2
- ## R
- Receipt header, 1-12-8
 - Receipt Language, 1-12-6
 - Receipt Layouts, **1-12-40**
 - Receipt Number, 1-10-14
 - Receipt texts
 - Germany, 1-15-53, 1-15-67
 - Norway, 1-15-37, 1-15-46
 - Poland, 1-15-61
 - Sweden, 1-15-13, 1-15-26
 - Receipts
 - Best Practice, 1-9-10
 - Description, 1-12-1
 - PCI, 1-7-3
 - Recipient and related indicator text, **1-12-24**
 - Reconciliation Indicator, 1-9-17, 1-9-18
 - Reference STAN, 1-9-21, 1-10-28, 1-12-18
 - Previous Transaction Status, 1-10-29
 - References, 1-4-8
 - Referral, Transaction Condition Codes, 1-12-16
 - Authorisation, 1-12-10
 - Refund, 1-12-10, 1-12-11, 1-12-21, 1-12-22, 1-12-24, 1-12-31
 - Application Selection, 1-9-4
 - Business Call, 1-11-21

- Functionalities, 1-10-6
 - Transaction Condition Codes, **1-12-16**
 - Regional Requirements, 1-15-1
 - Denmark, 1-15-4
 - Finland, 1-15-40
 - Germany, 1-15-48
 - Norway, 1-15-28
 - Poland, 1-15-55
 - Sweden, 1-15-15
 - Release of the ICC, Best Practice, 1-9-8
 - Report Segmentation, **1-9-19**
 - Reports, 1-14-24
 - PIN, 1-14-23
 - Digit, Representation, **1-14-19**
 - Management, 1-14-18
 - Restaurant, DCC, 1-10-80
 - Restaurants, 1-6-1
 - Retail Environment, Introduction, 1-6-1
 - Reversal (Auth.), Business Call, 1-11-21
 - RFU, Abbreviations, 1-4-2
 - RID, Abbreviations, 1-4-2
- ## S
- SAM, Abbreviations, 1-4-2
 - Scanned Bar Code Data, Prepaid MSC, **1-10-51**
 - SD, 1-11-18
 - SDA, Abbreviations, 1-4-2
 - SE Processing Code, Issuer Information Envelope, 1-15-20
 - Search Keys, Previous Transaction Status, 1-10-28
 - Secure Cryptographic Device, 1-14-18
 - Definition, 1-14-18
 - Secure Device, 1-11-18, 1-14-19
 - Secure Handling of PINs, Denmark, 1-15-4
 - Selectable Kernel Configurations, 1-10-19
 - Service Code, 1-14-15
 - Service Packs, Best Practice, 1-9-3
 - Service Packs requested, 1-14-2
 - Signature accepted?, Best Practice, 1-9-10
 - Signature Information, Receipts, 1-12-19
 - Signature on File, 1-10-64
 - Signature Validation, Best Practice, 1-9-11
 - Signature Verification and Accept, 1-9-10
 - Single Unit Terminal Terms, 1-4-4
 - Transaction Flow, **1-13-3**
 - SPA, 1-14-18
 - Special Functions, 1-10-78
 - Standard Receipt Layout, 1-12-6
 - Status of Previous Transaction, 1-10-28
 - Status of Previous Transactions, 1-10-28
 - Status of Previous Transactions (Terminal), Best Practice, 1-9-12
 - Stop List, Best Practice, 1-9-7
 - String, Notation, 1-4-6
 - Supplementary Authorization Business Call, 1-11-21
 - Functionalities, 1-10-5
 - Support of Card Technologies, Best Practice, 1-9-3
 - Support of Cardholder Verification Methods, Best Practice, 1-9-4
 - Surcharges, Best Practice, 1-9-13
 - Swedish regional receipt requirements, 1-15-18
- ## T
- Tag
 - 4F, 1-12-17
 - 4O, 1-10-14
 - 4P, 1-10-15
 - 4Q, 1-10-15
 - 4R, 1-10-15
 - 50, 1-12-14, 1-14-14
 - 5F34, 1-12-17
 - 545A, 1-15-20
 - 5A32, 1-15-20
 - 5A33, 1-15-20
 - 5A34, 1-15-20
 - 5A36, 1-15-20
 - 5A37, 1-15-20
 - 5A38, 1-15-20
 - 5A41, 1-15-20
 - 5F25, 1-12-17
 - 5F2D, 1-15-3
 - 5F57, 1-10-15
 - 9F11, 1-14-14
 - 9F12, 1-14-14
 - 9F1A, 1-10-27
 - C4, 1-9-21
 - C9, 1-9-26
 - D1, 1-9-21

- D2, 1-9-24
- DF60, 1-10-27
- DF61, 1-10-27
- DF62, 1-10-27
- DF63, 1-10-27
- DF64, 1-10-27
- DF65, 1-10-27
- DF66, 1-10-27
- DF6C, 1-10-27
- E3, 1-10-27
- E6, 1-10-48
- M4, 1-10-48
- TAPA, 1-5-2
- TC, Abbreviations, 1-4-2
- Temporary Offline Procedure, Best Practice, 1-9-5
- Terminal Categories, Best Practice, 1-9-1
- Terminal Decision Flags, AID Selection Table, 1-14-7
- Terminal functions
 - DCC, 1-10-65
 - Sweden, 1-15-16
- Terminal Handlers, 1-14-16
- Terminal Key, DCC, 1-10-62
- Terminal Operator, 1-6-2
 - Terms, 1-4-5
- Terminal Profiles, 1-14-1
- Terminal Services, 1-10-11
- Terminal Software version no., 1-14-2
- Terminal Supplier, 1-14-21
 - Terms, 1-4-5
- Terminal Type, 1-6-1
- Terminal Types, **1-6-7**
- Terminal Types and Environments, 1-6-1
- Terminals with
 - Combined Cardholder and Merchant Interface, Attachment S, 1-13-1
- Terms, Translation, 1-11-20
- Test House, Terms, 1-4-5
- Text Key, DCC, 1-10-62
- Text Written in Grey, Notation, 1-4-6
- The Card Handler, General Requirements, 1-14-17
- Time-out, 1-15-2
- Time-out value, Duplicate Transaction Check, 1-9-12
- Time, local transaction, 1-9-17
- Timing attack, 1-14-18
- Tip, Regional Requirements, 1-15-5
- Tips, Sweden, 1-15-15
- Tips/Gratuity
 - DCC, 1-10-80
 - Functionalities, 1-10-96
- Token, Terms, 1-4-5
- Token based Transaction Types, 1-10-59
- Token Date, DCC, 1-10-62
- Token Management Functions, DCC, 1-10-64
- Token transactions, Functionalities, 1-10-57
- Top Up, Business Call, 1-11-21
- Total Reports
 - DCC, 1-9-25
 - Description, 1-9-16
- Track 2, 1-9-3
- Track 3, 1-9-3
- Track2 Data, PCI, 1-7-5
- Transaction, Terms, 1-4-5
- Transaction and related header text, Receipts, **1-12-10**
- Transaction Checks, Best Practice, 1-9-12
- Transaction Condition Codes, **1-12-16**
- Transaction Information, Receipts, 1-12-13
- Transaction Log, 1-7-3
- Transaction Requests and Totals Affected, **1-9-20**
- Transaction Requirements when using a PSAM, 1-14-26
- Transaction Result, Best Practice, 1-9-11
- Transaction State Information, Best Practice, 1-9-26
- Transaction Type and Amount Elements, Receipts, **1-12-31**
- Transaction Type and Exchange Rate Type, Receipts, **1-12-27**
- Transaction Types, Previous Transaction Status, 1-10-31
- Transmission Speed, 1-9-9
- TRG, Abbreviations, 1-4-2
- Truncation of PAN digits, **1-12-15**
- Truncation of the PAN, PCI, 1-7-3
- Type of application, 1-14-2

U

UPT, 1-4-5

Abbreviations, 1-4-2

User Interface Display, Description,
1-11-1

User Interface Handler
Cardholder Display, 1-14-20
PIN Pad, 1-14-18

V

Value Added Tax, Receipts, 1-12-12

VAT, 1-10-16

VAT Amount, Issuer Information Envelope, 1-15-20

Visa/Dankort, Terms, 1-4-5

Voice Authorization, Definition, 1-4-5

Voice Authorization Call, Single Unit Terminal, 1-13-8

Voice Authorization Calls, 1-9-6

VPKI, Abbreviations, 1-4-2

W

Websites, 1-4-13

Write Handler String command, 1-10-58

This page is intentionally left blank



**Technical Reference Guide,
Open Terminal Requirement
Specification - Book 2**

Technical Interface

2013-11-15

VERSION 3.3.4

This page is intentionally left blank

How to Contact Nets Denmark A/S

Contact addresses are found on www.nets.eu

Disclaimers

Copyright Information

This document contains information proprietary to Nets Denmark A/S. The information, whether in the form of e.g. text, schematics, tables, drawings or illustrations, must not, without the prior, written consent of Nets Denmark A/S, be copied, reproduced or otherwise duplicated, disclosed outside the recipient company or organization or used by the recipient for purposes other than those explicitly agreed in writing with Nets Denmark A/S.

This limitation does not limit the recipient's right to duplicate and use information contained in the document if such information is received from another source without restriction provided such source is not in breach of an obligation of confidentiality towards Nets Denmark A/S.

Trademarks

PBS, the PBS-logo and the Nets logo are registered trademarks of Nets Denmark A/S. Dankort, VISA, Eurocard, MasterCard and Maestro names and logos are registered trademarks of Nets Denmark A/S and its international partners.

Limitation of Liability

Under no circumstances shall Nets Denmark A/S be liable for any direct incidental, indirect, special or consequential damages whatsoever (including but not limited to lost profits) arising out of or relating to this document or the information contained in it, even if Nets Denmark A/S has been advised, knew or should have known of the possibility of such damages.

Disputes

Any disputes arising from information contained in this document or work relating hereto will be settled in the Danish courts in accordance with Danish law.

Certification

Any new or updated type of Terminal must be certified by Nets Denmark A/S before being installed at Merchant locations and being prepared for transmission of transactions to Nets Denmark A/S.

This page is intentionally left blank

2-1 Table of Contents

Technical Reference Guide, Open Terminal Requirements Specification - Book 2 i
2-1 Table of Contents	2-1-1
2-2 Revision Log, Book 2	2-2-1
2-3 System Overview	2-4-1
2-3.1 Terminal Model	2-4-1
2-3.1.1 Terminal Architecture for PSAM Applications (TAPA)	2-4-1
2-3.2 A Physical Implementation of the TAPA Model	2-4-2
2-3.2.1 Merchant Application	2-4-3
2-3.2.2 The MAD-Handler	2-4-4
2-3.2.3 Card Readers (General)	2-4-4
2-3.2.4 Magnetic Stripe Card Reader	2-4-4
2-3.2.5 Integrated Circuit Card Reader	2-4-4
2-3.2.6 PIN Entry Device (PED)	2-4-5
2-3.2.7 Displays	2-4-5
2-3.2.8 Receipt Printer	2-4-5
2-3.2.9 Command Keys	2-4-5
2-3.2.10 Data Store	2-4-6
2-3.2.11 Logging Devices	2-4-6
2-3.2.12 Transfer of Stored Debit/Credit Transactions	2-4-6
2-3.2.13 The Interface to the PSAM and the PSAM functions	2-4-6
2-3.3 Application Selection	2-4-8
2-3.4 Security Zones, Debit/Credit	2-4-9
2-4 General Requirements	2-4-1
2-4.1 Introduction	2-4-1
2-4.1.1 Related Specifications	2-4-1
2-4.2 Card Related Transactions	2-4-1
2-4.2.1 Transaction flow	2-4-1
2-4.2.2 Cancellation	2-4-3
2-4.3 Tokens	2-4-3
2-4.3.1 Format and Retrieval of the Token	2-4-3
2-4.3.2 The use of Tokens	2-4-4
2-4.4 Cardholder Verification	2-4-5
2-4.4.1 PIN Entry	2-4-5
2-4.4.2 Signature	2-4-5
2-4.5 The Router	2-4-6
2-4.5.1 Functional Requirements	2-4-6
2-4.5.2 Command Flow	2-4-6
2-4.6 Multi-Application Driver Handler (MAD-Handler)	2-4-6
2-4.6.1 General Requirements	2-4-6
2-4.7 Card Handler	2-4-7
2-4.7.1 General Requirements	2-4-7
2-4.7.2 Magnetic Stripe Card Reader (MSCR)	2-4-7
2-4.7.3 ICCR - General	2-4-9
2-4.7.4 ICCR - Processor Card Reader	2-4-9

2-4.8	User Interface Handler	2-4-10
2-4.8.1	Cardholder Display	2-4-10
2-4.8.2	Audio Indicator	2-4-14
2-4.8.3	Cardholder Key Pad	2-4-14
2-4.8.4	Printer	2-4-14
2-4.9	Merchant Application Handler	2-4-14
2-4.9.1	Log	2-4-14
2-4.9.2	Serial Ports	2-4-15
2-4.9.3	Merchant Display	2-4-15
2-4.10	PSAM Handler	2-4-16
2-4.10.1	Interface to the PSAM	2-4-16
2-4.10.2	Commands between the CAD and the PSAM	2-4-18
2-4.11	Data Store Handler	2-4-18
2-4.11.1	Data Store	2-4-18
2-4.12	Communication Handler	2-4-18
2-4.12.1	General Requirements	2-4-18
2-4.13	Event Handler	2-4-19
2-4.13.1	General Requirements	2-4-19
2-4.14	New PIN Synchronization	2-4-19
2-4.14.1	General Requirements	2-4-19
2-4.14.2	Key Generation Requirements	2-4-19
2-4.14.3	Key derivation	2-4-20
2-4.15	Card Data Protection	2-4-21
2-4.15.1	Introduction	2-4-21
2-4.15.2	CDP Implementation	2-4-21
2-4.15.3	Key Mgmt - KEYCDP from a secure Card Reader	2-4-21
2-4.15.4	Enabling CDP mode in the PSAM	2-4-22
2-4.15.5	Generating of CDP Session Key (KSESCDP)	2-4-22
2-4.15.6	Using the KSESCDP	2-4-22
2-4.15.7	Private Label MSC recognition in CDP mode	2-4-22
2-4.15.8	Get Last ICC Response handling in CDP mode	2-4-22
2-4.15.9	Verify Offline PIN handling in CDP mode	2-4-23
2-4.15.10	Check Stop List handling in CDP mode	2-4-23
2-4.16	Terminal Initialization	2-4-23
2-4.16.1	Reset of the CAD	2-4-23
2-4.17	Fallback from ICC to Magnetic Stripe	2-4-24
2-4.17.1	Introduction	2-4-24
2-4.17.2	General Requirements	2-4-24
2-4.17.3	Final Decision	2-4-26
2-4.18	Counters and Batch Numbers	2-4-34
2-4.18.1	Introduction	2-4-34
2-4.18.2	Batch Number	2-4-34
2-5	Debit/Credit Functionality	2-5-1
2-5.1	Application Initialization	2-5-1
2-5.1.1	Introduction	2-5-1
2-5.1.2	Power On	2-5-2
2-5.1.3	Restart	2-5-6
2-5.1.4	Installation	2-5-10
2-5.1.5	New Application Data	2-5-10
2-5.1.6	Configuration	2-5-11
2-5.1.7	PSAM/PIN Pad Synchronization	2-5-12
2-5.1.8	PSAM Shutdown	2-5-14

2-5.2	Stop List	2-5-14
2-5.2.1	Data Values used for Stop List Status	2-5-14
2-5.3	Technology independent requirements	2-5-16
2-5.3.1	Transaction Processing	2-5-16
2-5.3.2	Initialization of the Transaction	2-5-16
2-5.3.3	Initiate xxx Payment	2-5-16
2-5.3.4	EMV/MSC/Key Entered/Token based Payment	2-5-18
2-5.3.5	Validate Data	2-5-18
2-5.3.6	Complete xxx Payment	2-5-19
2-5.4	Requirements common to EMV, MSC and KE Trans. ..	2-5-20
2-5.4.1	Transaction Processing	2-5-20
2-5.4.2	Initialization of the EMV/MSC/KE Payment Trans. ..	2-5-20
2-5.4.3	Initiate EMV/MSC/Key Entered Payment	2-5-20
2-5.4.4	EMV/MSC/Key Entered Payment	2-5-21
2-5.4.5	Validate Data	2-5-22
2-5.4.6	Complete EMV/MSC/Key Entered Payment	2-5-22
2-5.5	EMV Card Transactions	2-5-23
2-5.5.1	Transaction Processing	2-5-23
2-5.5.2	Initialization of the EMV Deb/Cred Payment Trans.	2-5-23
2-5.5.3	Initiate EMV Payment	2-5-23
2-5.5.4	EMV Payment	2-5-25
2-5.5.5	Validate Data	2-5-26
2-5.5.6	Complete EMV Payment	2-5-27
2-5.5.7	EMV-related Data Elements	2-5-27
2-5.6	Optimizing the Transaction Time, EMV	2-5-29
2-5.6.1	Introduction	2-5-29
2-5.6.2	Accelerated PIN Entry	2-5-29
2-5.6.3	Release of the ICC	2-5-31
2-5.7	Magnetic Stripe Card Transactions	2-5-45
2-5.7.1	Transaction Processing	2-5-45
2-5.7.2	Initialization of the MSC Deb/Cred Payment Trans.	2-5-45
2-5.7.3	Initiate MSC Payment	2-5-46
2-5.7.4	MSC Payment	2-5-47
2-5.7.5	Validate Data	2-5-47
2-5.7.6	Complete Payment	2-5-47
2-5.8	Key Entered Card Transactions	2-5-62
2-5.8.1	Transaction Processing	2-5-62
2-5.8.2	Initialization of the KE Deb/Cred Payment Trans. ..	2-5-63
2-5.8.3	Initiate Key Entered Payment	2-5-63
2-5.8.4	Key Entered Payment	2-5-63
2-5.8.5	Validate Data	2-5-64
2-5.8.6	Complete Key Entered Payment	2-5-64
2-5.9	Token based Transactions	2-5-72
2-5.9.1	Transaction Processing	2-5-72
2-5.9.2	Initialization of the Token Deb/Cred Payment Trans	2-5-73
2-5.9.3	Initiate Token Based Payment	2-5-73
2-5.9.4	Token Based Payment	2-5-74
2-5.9.5	Validate Data	2-5-74
2-5.9.6	Complete Token Based Payment	2-5-75
2-5.10	Cancellation	2-5-84
2-5.10.1	Introduction	2-5-84
2-5.10.2	Transaction Flow	2-5-84

2-5.11	Post Registration	2-5-86
2-5.11.1	Introduction	2-5-86
2-5.11.2	Transaction Flow	2-5-86
2-5.12	Addendum Records	2-5-87
2-5.12.1	Introduction	2-5-87
2-5.12.2	Handling of Addendum Records	2-5-87
2-5.13	Administrative Transactions and Processes	2-5-91
2-5.13.1	Introduction	2-5-91
2-5.13.2	Installation Transaction	2-5-91
2-5.13.3	PSAM Update Transaction	2-5-93
2-5.13.4	PSAM Deactivation Transaction	2-5-96
2-5.13.5	Clock Synchronization	2-5-97
2-5.14	Online Transactions	2-5-97
2-5.14.1	PSAM Update Flag	2-5-98
2-5.14.2	PSAM Scripts	2-5-98
2-5.14.3	Repeat Messages	2-5-98
2-5.14.4	Communication Session	2-5-99
2-5.14.5	Terminal Operator Communication Access Points ..	2-5-100
2-5.15	Transferring Advices	2-5-101
2-5.15.1	General Principles	2-5-101
2-5.15.2	The Transfer of Advices	2-5-101
2-5.15.3	Advice Transfer	2-5-104
2-5.15.4	Security Mechanism	2-5-106
2-5.15.5	Advice Window Size	2-5-107
2-5.15.6	Counters and Batch Numbers	2-5-109
2-5.15.7	Exception condition - Accumulated Advices	2-5-110
2-5.15.8	Exception Conditions, Failed Delivery of Advices	2-5-111
2-5.16	Exception Handling	2-5-115
2-5.16.1	General Rules	2-5-115
2-5.16.2	Categories	2-5-117
2-5.16.3	Terminal Related Errors	2-5-117
2-5.16.4	PSAM Related Errors	2-5-118
2-5.16.5	Host Declined Transactions (Requests)	2-5-119
2-5.16.6	Application Status Words	2-5-122
2-5.16.7	PSAM Declined Online Transactions	2-5-122
2-5.16.8	PSAM Declined Offline Transactions	2-5-122
2-5.16.9	Card Declined Transactions	2-5-122
2-5.16.10	Cardholder Initiated Actions	2-5-122
2-5.16.11	Communication Statistics and Error Counters	2-5-123
2-5.16.12	Authorization Advice	2-5-123
2-5.16.13	Message Codes	2-5-123
2-5.16.14	Action Codes	2-5-124
2-5.16.15	Merchant Initiated Actions	2-5-125
2-5.16.16	Time-outs	2-5-126
2-6 Design Requirements	2-6-1	
2-6.1	General Considerations	2-6-1
2-6.1.1	Environmental Requirements	2-6-1
2-6.1.2	Documentation	2-6-1
2-6.1.3	Marking	2-6-2
2-6.1.4	Servicing the Terminal	2-6-3
2-6.2	Mechanical Design	2-6-3
2-6.2.1	General Requirements	2-6-3
2-6.2.2	Combined Card Reader	2-6-3

2-6.2.3	Integrated Circuit Card Reader	2-6-4
2-6.2.4	Magnetic Stripe Card Reader	2-6-4
2-6.2.5	Visual Indicators	2-6-4
2-6.2.6	Audio Indicator	2-6-5
2-6.2.7	Cardholder Keyboard	2-6-6
2-6.2.8	PIN Pad	2-6-6
2-6.2.9	Command Keys	2-6-8
2-6.2.10	Receipt Printer	2-6-9
2-6.3	Electrical Design	2-6-9
2-6.3.1	Introduction	2-6-9
2-6.3.2	General Requirements	2-6-9
2-6.3.3	Data Store	2-6-9
2-6.4	Software Design	2-6-10
2-6.4.1	Introduction	2-6-10
2-6.4.2	General Requirements	2-6-10
2-6.4.3	Additional Requirements to the PED Software	2-6-10
2-6.4.4	Data Management	2-6-10
2-6.4.5	Storage of Data	2-6-11
2-6.4.6	Storage of Software	2-6-11
2-6.4.7	Download Requirements	2-6-11
2-6.5	Chip Card Reader Design Requirements	2-6-12
2-6.5.1	PSAM Card Reader(s)	2-6-12
2-6.5.2	Electrical Interfaces	2-6-13
2-7	Privacy Shield on PIN Entry Devices, PED	2-7-1
2-7.1	Introduction	2-7-1
2-7.1.1	Terminology	2-7-1
2-7.2	Privacy Shield around the PED	2-7-2
2-7.2.1	Shielding - Size and Orientation	2-7-2
2-7.2.2	PED and Additional Numeric Keys	2-7-3
2-7.3	Shielding - Design Recommendations	2-7-3
2-7.3.1	Introduction	2-7-3
2-7.4	Protected access to Card Reader and PED	2-7-4
2-7.4.1	Access to the interior of the terminal	2-7-5
2-7.4.2	No operation when the terminal is open	2-7-6
2-7.4.3	Other Equipment	2-7-7
2-7.5	Figures	2-7-8
2-7.5.1	Privacy Shield around the PED	2-7-8
2-7.5.2	Reference Directions	2-7-9
2-7.5.3	The Height of the Shielding	2-7-10
2-7.5.4	Mounting of the PED (Angle)	2-7-11
2-7.5.5	Height and position of the PED	2-7-12
2-8	Service Packs	2-8-1
2-8.1	Introduction	2-8-1
2-8.2	Selection of Service Packs supported	2-8-1
2-8.2.1	General requirements	2-8-1
2-8.2.2	Terminal - Terminal Approval No.	2-8-1
2-8.3	Service Packs Overview	2-8-2
2-8.4	Service Pack No. 1	2-8-3
2-8.4.1	MSC PIN Retry	2-8-3
2-8.4.2	Get Amount 2	2-8-3
2-8.4.3	Validate Data 2	2-8-4

2-8.5	Service Pack No. 2	2-8-5
2-8.5.1	Get Amount 3	2-8-5
2-8.5.2	Message Size	2-8-6
2-8.5.3	Issuer Envelope Functionality	2-8-7
2-8.5.4	Initiate Payment 2 / Account Type	2-8-8
2-9	Merchant Initiative Bypass	2-9-1
2-9.1	General	2-9-1
2-9.1.1	Introduction	2-9-1
2-9.1.2	General Requirements	2-9-1
2-10	Additional Transaction Information	2-10-1
2-10.1	Introduction	2-10-1
2-10.2	Flex Terminals and Transaction Information	2-10-1
2-10.2.1	Terminal requirements	2-10-2
2-11	Private Label Card Schemes	2-11-1
2-11.1	Handling of Private Label Cards	2-11-1
2-11.1.1	Introduction	2-11-1
2-11.1.2	Description	2-11-1
2-11.1.3	Flow	2-11-1
2-12	Local PIN	2-12-1
2-12.1	Local PIN Validation Message Flow	2-12-1
2-12.1.1	Introduction	2-12-1
2-12.1.2	Description	2-12-1
2-12.1.3	Local PIN Validation	2-12-2
2-12.2	Plaintext PIN Data	2-12-4
2-12.2.1	Local PIN Validation command - Plaintext PIN	2-12-4
2-12.3	Enciphered PIN Data	2-12-4
2-12.3.1	Key Management	2-12-4
2-12.3.2	Load LP Keys Command	2-12-6
2-12.3.3	Local PIN Validation command - Enciphered PIN ...	2-12-7
2-12.3.4	Get Debit/Credit Properties Command	2-12-10
2-12.3.5	Complete Payment Command	2-12-10
2-12.4	Limitations	2-12-10
2-12.4.1	En./Dis. of the Local PIN Validation functionality ...	2-12-10
2-12.4.2	Availability of the Local PIN Validation functionality	2-12-10
2-12.4.3	PIN Range	2-12-10
2-12.4.4	PIN tries	2-12-10
2-12.5	Application Status Words (ASW1-ASW2)	2-12-11
2-12.6	Message Codes	2-12-11
2-12.7	Example of Message Flow	2-12-11
2-13	Host Communication - Protocols and Formats	2-12-1
2-13.1	Introduction	2-12-1
2-13.2	General	2-12-1
2-13.3	Communication Protocols	2-12-2
2-13.3.1	Physical Layer	2-12-2
2-13.3.2	Data Link Layer	2-12-3
2-13.3.3	Network Layer	2-12-3
2-13.3.4	Transport Layer	2-12-3

2-13.3.5	Session Layer	2-12-3
2-13.3.6	Presentation and Application Layers	2-12-3
2-13.4	Transmission Flows	2-12-3
2-13.5	Transmission Formats	2-12-4
2-13.5.1	APACS Message Types	2-12-4
2-13.5.2	APACS Message Header	2-12-5
2-13.6	Communication Statistics and Error Counters	2-12-12
2-13.6.1	Introduction	2-12-12
2-13.6.2	Communication Interface Statistics	2-12-12
2-13.6.3	Error Counters	2-12-12
2-13.6.4	Error Counters, tag TE, TF, TG and TH	2-12-13
2-13.7	Primitive Data Objects for the APACS Header	2-12-14
2-13.7.1	Coding of Tag 'C0' (Length of APACS 60 Message) ..	2-12-14
2-13.7.2	Coding of Tag 'C1' (Message Type Identifier)	2-12-14
2-13.7.3	Coding of Tag 'C2' (Function Code)	2-12-14
2-13.7.4	Coding of Tag 'C3' (PSAM Identifier)	2-12-14
2-13.7.5	Coding of Tag 'C4' (Systems Trace Audit Number) ..	2-12-14
2-13.7.6	Coding of Tag 'C5' (KEKDATA)	2-12-14
2-13.7.7	Coding of Tag 'C6' ([KSESDATA])	2-12-14
2-13.7.8	Coding of Tag 'C7' (APACS MAC Key Version)	2-12-14
2-13.7.9	Coding of Tag 'C8' (Advice Window Size)	2-12-15
2-13.7.10	Coding of Tag 'C9' (PSAM Update Flag)	2-12-15
2-13.7.11	Coding of Tag 'CA' (Display Line for Host Message)	2-12-15
2-13.7.12	Coding of Tag 'CB' (Network Connection Type)	2-12-15
2-13.7.13	Coding of Tag 'CC' (MAD-Handler ID)	2-12-16
2-13.7.14	Coding of Tag 'CD' (Terminal Identification)	2-12-16
2-13.7.15	Coding of Tag 'CE' (Proprietary Data)	2-12-16
2-13.7.16	Coding of Tag 'CF' (Communication Interface Statistics)	2-12-16
2-13.7.17	Coding of Tag 'D1' (Reference STAN)	2-12-17
2-13.7.18	Coding of Tag 'D2' (MTI of the Original Message) ..	2-12-17
2-13.8	Detailed Message Formats	2-12-19
2-13.8.1	Authorization Request Messages (0106/0116)	2-12-19
2-13.8.2	Authorization Advice Messages (0126/0136)	2-12-26
2-13.8.3	Financial Request Messages (0206/0216)	2-12-32
2-13.8.4	Financial Advice Messages (0226/0236)	2-12-38
2-13.8.5	PSAM Upd. & Recon. Msg. (0360/364/0370/374) ..	2-12-45
2-13.8.6	Reversal Advice Messages (0426/0436)	2-12-47
2-13.8.7	Addendum Record Messages (0624/0634)	2-12-55
2-13.8.8	Service Record Messages (0624/0634)	2-12-56
2-13.8.9	Clock Synchronization Messages (0804/0814)	2-12-57
2-13.8.10	Installation Messages (0804/0814)	2-12-58
2-13.8.11	Advice Transfer Messages (0804/0814)	2-12-60
2-13.8.12	PSAM Update Messages (0804/0814/0844)	2-12-61
2-13.8.13	PSAM Deactivation Messages (0804/0814)	2-12-62
2-13.8.14	Reconciliation Messages (0804/0814/844)	2-12-63
2-13.9	Coding of Application Specific Fields	2-12-65
2-13.9.1	Coding Conventions	2-12-65
2-13.9.2	Coding of Field 3 (Processing Code)	2-12-65
2-13.9.3	Coding of Field 15 (GMT Offset)	2-12-66
2-13.9.4	Coding of Field 21 (POS Capability Code)	2-12-66
2-13.9.5	Coding of Field 22 (POS Entry Mode)	2-12-70
2-13.9.6	Coding of Field 24 (Function Code)	2-12-79
2-13.9.7	Coding of Field 25 (Message Reason Code)	2-12-80

2-13.9.8	Coding of Field 27 (Download Control)	2-12-82
2-13.9.9	Coding of Field 39 (Action Code)	2-12-82
2-13.9.10	TLV Coding of Field 44 (Additional Response Data)	2-12-86
2-13.9.11	TLV Coding of Field 46 (CAD Mgmt/Svc. Qual. Data)	2-12-87
2-13.9.12	Coding of Field 47 (Additional Data - National)	2-12-89
2-13.9.13	Coding of Field 55 (ICC System Related Data)	2-12-89
2-13.9.14	Coding of Field 56 (Original Data Elements)	2-12-91
2-13.9.15	Coding of Field 59 (Additional Data Capture)	2-12-91
2-13.9.16	Coding of Field 60 (PSAM Identifier)	2-12-92
2-13.9.17	Coding of Field 61 (Random Number)	2-12-93
2-13.9.18	Coding of Field 62 (Merchant Initiative)	2-12-93
2-13.9.19	TLV Coding of Field 63 (PSAM Upd./Recon. Data)	2-12-93
2-13.9.20	Coding of Field 71 (Message Number)	2-12-93
2-13.9.21	TLV Coding of Field 72 (Addendum Record)	2-12-94
2-14	Commands and Responses	2-14-1
2-14.1	Introduction	2-14-1
2-14.2	Command Overview	2-14-1
2-14.3	Error Responses	2-14-7
2-14.3.1	MAD-Handler Interface to the PSAM	2-14-7
2-14.4	Commands used during Initialization	2-14-8
2-14.4.1	Start-up PSAM	2-14-8
2-14.4.2	Get Supported AIDs	2-14-9
2-14.4.3	Get MSC Table	2-14-11
2-14.4.4	Get Debit/Credit File Characteristics	2-14-13
2-14.4.5	Configure PSAM Application	2-14-15
2-14.4.6	Synchronize PSAM/PIN Pad	2-14-16
2-14.4.7	Get Next	2-14-17
2-14.4.8	Exchange Debit/Credit Static Information	2-14-18
2-14.5	Debit/Credit Administrative Commands	2-14-20
2-14.5.1	Install	2-14-20
2-14.5.2	Install 2	2-14-21
2-14.5.3	Validate Install Data	2-14-23
2-14.5.4	Submit Initial Key 2	2-14-24
2-14.5.5	Add Addendum Record	2-14-26
2-14.5.6	Deactivate PSAM	2-14-27
2-14.5.7	Create Service Record	2-14-28
2-14.5.8	Get Debit/Credit Properties	2-14-29
2-14.5.9	Set Debit/Credit Properties	2-14-41
2-14.5.10	Get Random Number	2-14-44
2-14.5.11	Get Key Check Value 2	2-14-46
2-14.5.12	Get Processing Condition Table	2-14-47
2-14.5.13	PSAM Update	2-14-52
2-14.6	Debit/Credit Transaction Commands	2-14-53
2-14.6.1	Initiate EMV Payment 2	2-14-54
2-14.6.2	EMV Payment	2-14-57
2-14.6.3	Validate Data 2	2-14-59
2-14.6.4	Complete Payment	2-14-65
2-14.6.5	Initiate MSC Payment 2	2-14-66
2-14.6.6	Initiate MSC Payment 3	2-14-68
2-14.6.7	MSC Payment	2-14-71
2-14.6.8	Complete Payment	2-14-73
2-14.6.9	Initiate Key Entered Payment	2-14-74
2-14.6.10	Initiate Key Entered Payment 2	2-14-76

2-14.6.11	Key Entered Payment	2-14-79
2-14.6.12	Complete Payment	2-14-81
2-14.6.13	Initiate Token Based Payment 2	2-14-82
2-14.6.14	Token Based Payment	2-14-85
2-14.6.15	Complete Payment	2-14-87
2-14.6.16	Initiate Contactless Payment	2-14-88
2-14.6.17	Validate Contactless Payment	2-14-93
2-14.6.18	Complete Contactless Payment	2-14-95
2-14.6.19	Check Stop List	2-14-97
2-14.6.20	Verify Signature	2-14-99
2-14.6.21	Get Merchant Data	2-14-100
2-14.6.22	Transaction State Information	2-14-102
2-14.6.23	Repeat Last ICC Response	2-14-104
2-14.6.24	Submit Card Reference	2-14-105
2-14.6.25	Submit Card Reference 2	2-14-107
2-14.6.26	Retrieve Card Data MSC	2-14-109
2-14.6.27	Retrieve Card Data ICC	2-14-111
2-14.6.28	Initiate PIN Entry 2	2-14-112
2-14.6.29	Get Amount 3	2-14-114
2-14.7	Cancellation	2-14-117
2-14.7.1	Initiate Cancellation Payment	2-14-117
2-14.7.2	Cancellation Payment	2-14-119
2-14.7.3	Complete Payment	2-14-120
2-14.8	Local PIN Commands	2-14-122
2-14.8.1	Load LP Keys Command - Method Number 1	2-14-122
2-14.8.2	Local PIN Validation	2-14-124
2-14.9	Card Data Protection	2-14-128
2-14.9.1	Load Card Data Protection Keys	2-14-128
2-14.10	ASW1-ASW2 Coding	2-14-130
2-14.10.1	App. Specific ASW1-ASW2 Coding (Debit/Credit) ...	2-14-131
2-14.10.2	ASW1-ASW2 Applicable for Local PIN	2-14-184
2-15	Data Elements	2-14-1
2-15.1	Introduction	2-14-1
2-15.1.1	Coding of Data Elements	2-14-1
2-15.1.2	Data Elements Defined in EMV and TAPA	2-14-1
2-15.2	Data Elements for the Debit/Credit Application	2-14-2
2-15.2.1	Account Type	2-14-2
2-15.2.2	Account Type Selection	2-14-2
2-15.2.3	Acquirer Name	2-14-2
2-15.2.4	Action Code	2-14-2
2-15.2.5	Action Indicator	2-14-3
2-15.2.6	Addendum Record	2-14-3
2-15.2.7	AID (Application Identifier)	2-14-3
2-15.2.8	Algorithm Id	2-14-4
2-15.2.9	ALGVLP	2-14-4
2-15.2.10	ALGVPPSYNC (Synch. Alg. and Key Length)	2-14-4
2-15.2.11	Amount	2-14-4
2-15.2.12	Amount, Other	2-14-4
2-15.2.13	Amount Request	2-14-5
2-15.2.14	Amount Status	2-14-5
2-15.2.15	Application Label	2-14-5
2-15.2.16	Approval Code	2-14-5
2-15.2.17	ASI (Application Selection Indicator)	2-14-5

2-15.2.18	Available Funds	2-14-6
2-15.2.19	AOSA (Available Offline Spending Amount)	2-14-6
2-15.2.20	Batch Number	2-14-6
2-15.2.21	BIB	2-14-6
2-15.2.22	BIB Amount	2-14-6
2-15.2.23	BIB Processing Code	2-14-7
2-15.2.24	Card Data	2-14-7
2-15.2.25	[Card Data]	2-14-7
2-15.2.26	Card Data Source	2-14-7
2-15.2.27	Card Name	2-14-7
2-15.2.28	Card Product Type	2-14-8
2-15.2.29	Card Reference	2-14-8
2-15.2.30	Card Sequence Number	2-14-8
2-15.2.31	Card Service Info	2-14-9
2-15.2.32	Cashback	2-14-9
2-15.2.33	CNTX (Count of X)	2-14-9
2-15.2.34	Contactless Terminal Settings	2-14-10
2-15.2.35	CURRC (Currency Code)	2-14-10
2-15.2.36	CURRE (Currency Exponent)	2-14-10
2-15.2.37	CV-2 (Card Verification, method 2)	2-14-11
2-15.2.38	CVM Status	2-14-11
2-15.2.39	Data Requested	2-14-12
2-15.2.40	DATEPCT	2-14-12
2-15.2.41	DCC Amount Extra (CH)	2-14-12
2-15.2.42	DCC Amount Goods & Services (ME)	2-14-12
2-15.2.43	DCC Amount Total (ME)	2-14-12
2-15.2.44	DCC Commission (CH)	2-14-13
2-15.2.45	DCC Commission (ME)	2-14-13
2-15.2.46	DCC CURR (ME)	2-14-13
2-15.2.47	DCC Indicator	2-14-13
2-15.2.48	DCC Mark Up Exchange Rate	2-14-13
2-15.2.49	DCC Reference Exchange Rate	2-14-14
2-15.2.50	DCC Reference Date	2-14-14
2-15.2.51	DCC Waiter ID	2-14-14
2-15.2.52	Default Kernel ID	2-14-14
2-15.2.53	Dual Card Reference	2-14-15
2-15.2.54	Duplicate Transaction Time-out	2-14-15
2-15.2.55	EMV Checksum	2-14-15
2-15.2.56	Error Code	2-14-16
2-15.2.57	Expiry Date	2-14-16
2-15.2.58	Expiry Date (Surface of the Card)	2-14-17
2-15.2.59	Extended Issuer Envelope Data	2-14-17
2-15.2.60	FILEIDADMIN	2-14-17
2-15.2.61	FILEIDPRIORITY,n	2-14-17
2-15.2.62	Final Card Balance	2-14-17
2-15.2.63	Hardware Version Number	2-14-17
2-15.2.64	Host Request	2-14-18
2-15.2.65	Host Response	2-14-18
2-15.2.66	IDPSAM (Identifier for a PSAM)	2-14-18
2-15.2.67	IDPSAMAPP (TAPA PSAM Application Identifier) ...	2-14-18
2-15.2.68	IDPSAMCREATOR	2-14-18
2-15.2.69	Info Level	2-14-18
2-15.2.70	Initial Card Balance	2-14-19
2-15.2.71	Issuer DD (Issuer Discretionary Data in FCI)	2-14-19
2-15.2.72	Issuer Envelope Data	2-14-19

2-15.2.73	Kernel ID	2-14-19
2-15.2.74	Kernel Version	2-14-20
2-15.2.75	Key Check Value (KCV)	2-14-20
2-15.2.76	Key Enter	2-14-21
2-15.2.77	LENX (Length of Field X)	2-14-21
2-15.2.78	Limit Info	2-14-21
2-15.2.79	Local PIN Verification Status	2-14-21
2-15.2.80	MAD-Handler ID	2-14-21
2-15.2.81	Magnetic Stripe Contents	2-14-22
2-15.2.82	Magstripe Indicator	2-14-22
2-15.2.83	Maximum Deposit	2-14-22
2-15.2.84	MDOL (MAD-Handler Data Object List)	2-14-22
2-15.2.85	MDOL Data	2-14-23
2-15.2.86	MEADDRESS (Merchant Address)	2-14-23
2-15.2.87	MEBRN (Business Registration Number)	2-14-23
2-15.2.88	MECITY (Merchant City Name)	2-14-23
2-15.2.89	MENAME (Merchant Name)	2-14-23
2-15.2.90	MENUMBER (Merchant Number)	2-14-23
2-15.2.91	MEPHONE (Merchant Phone No.)	2-14-24
2-15.2.92	MEZIP (Merchant Postal Code)	2-14-24
2-15.2.93	MI (Merchant Initiative)	2-14-24
2-15.2.94	Mode	2-14-26
2-15.2.95	MTI (Message Type Identifier)	2-14-26
2-15.2.96	MTI of the Original Message	2-14-26
2-15.2.97	PAN (Primary Account Number)	2-14-26
2-15.2.98	PAN Sequence Number	2-14-27
2-15.2.99	PANFROM	2-14-27
2-15.2.100	PANTO	2-14-27
2-15.2.101	Payment Conditions	2-14-27
2-15.2.102	PCI Data	2-14-27
2-15.2.103	PCT PANFROM	2-14-28
2-15.2.104	PCT PANTO	2-14-28
2-15.2.105	PIN Block Format	2-14-28
2-15.2.106	PIN Data	2-14-29
2-15.2.107	POS Capability Code	2-14-29
2-15.2.108	POS Entry Mode	2-14-29
2-15.2.109	PSAM Code Checksum	2-14-29
2-15.2.110	PSAM Config Checksum	2-14-30
2-15.2.111	PSAM D/C Life Cycle State	2-14-30
2-15.2.112	PSAM Parameters	2-14-30
2-15.2.113	PSAM Security Configuration	2-14-30
2-15.2.114	PSAM Subversion	2-14-31
2-15.2.115	PSAM Version	2-14-31
2-15.2.116	PTS Request Data	2-14-31
2-15.2.117	PTS Response Data	2-14-32
2-15.2.118	RandomNUMBER	2-14-33
2-15.2.119	RECON_CounterID	2-14-33
2-15.2.120	RECON_CounterNAME	2-14-33
2-15.2.121	RECON_PANFROM	2-14-34
2-15.2.122	RECON_PANTO	2-14-34
2-15.2.123	Reference STAN	2-14-34
2-15.2.124	RIDPSAM	2-14-34
2-15.2.125	Salt	2-14-34
2-15.2.126	Salt Version	2-14-35
2-15.2.127	Scheme Id	2-14-35

2-15.2.128	Scheme Id Bitmap	2-14-35
2-15.2.129	Seed	2-14-35
2-15.2.130	Selectable Kernel Configurations	2-14-35
2-15.2.131	Service Code	2-14-36
2-15.2.132	Service Packs Supported	2-14-36
2-15.2.133	SettingsCL	2-14-36
2-15.2.134	Signature Verification	2-14-37
2-15.2.135	Software Version Number	2-14-37
2-15.2.136	STAN (System Trace Audit Number)	2-14-37
2-15.2.137	Statistics	2-14-38
2-15.2.138	Stop List Status	2-14-38
2-15.2.139	SUBVERSIONPCT	2-14-38
2-15.2.140	TAGAdditionalInfo	2-14-38
2-15.2.141	Terminal Approval No.	2-14-38
2-15.2.142	Terminal Checksum	2-14-39
2-15.2.143	Terminal Contactless Floor Limit	2-14-39
2-15.2.144	Terminal Contactless Transaction Limit	2-14-39
2-15.2.145	Terminal CVM Required Limit	2-14-39
2-15.2.146	Terminal Decision Flags	2-14-40
2-15.2.147	Terminal Identification	2-14-40
2-15.2.148	Terminal Manufacturer ID	2-14-40
2-15.2.149	Terminal Serial Number	2-14-41
2-15.2.150	Terminal Settings	2-14-41
2-15.2.151	Token	2-14-41
2-15.2.152	[Track Data]	2-14-42
2-15.2.153	Track1 Data	2-14-42
2-15.2.154	Track2 Data	2-14-42
2-15.2.155	Track3 Data	2-14-42
2-15.2.156	Transaction Category Code	2-14-42
2-15.2.157	Transaction Gratuity Amount	2-14-43
2-15.2.158	Transaction Identifier (TI)	2-14-43
2-15.2.159	Transaction Request (TR)	2-14-43
2-15.2.160	Transaction Options (TO)	2-14-44
2-15.2.161	Transaction State Information	2-14-44
2-15.2.162	Transaction Status	2-14-45
2-15.2.163	Transaction Total Amount	2-14-45
2-15.2.164	Transaction Type (TT)	2-14-45
2-15.2.165	Truncated PAN	2-14-45
2-15.2.166	TSPED KEK	2-14-46
2-15.2.167	TSPSAMKEK	2-14-46
2-15.2.168	Type of Application	2-14-46
2-15.2.169	Update Data	2-14-46
2-15.2.170	Update Number	2-14-46
2-15.2.171	VAT Amount	2-14-46
2-15.2.172	VERSIONPCT	2-14-46
2-15.2.173	VKBDK(Base Derivation Key Version)	2-14-47
2-15.2.174	VKPED KEK(KEK Version, PED)	2-14-47
2-15.2.175	VKPSAM KEK(KEK Version, PSAM)	2-14-47
2-15.3	Data Elements specific to the Local PIN Application	2-14-48
2-15.3.1	Key Check Value (KCV)	2-14-48
2-15.3.2	Last PIN incorrect	2-14-48
2-15.3.3	LP-KEK	2-14-48
2-15.3.4	LP-KEK-Version	2-14-48
2-15.3.5	LP-Key	2-14-48
2-15.3.6	LP-Key-Chain	2-14-49

2-15.3.7	LP-Key-Version	2-14-49
2-15.3.8	Maximum PIN digits	2-14-49
2-15.3.9	Method Number	2-14-49
2-15.3.10	Minimum PIN digits	2-14-49
2-15.3.11	Number of PIN tries left	2-14-49
2-15.3.12	Time	2-14-50
2-15.3.13	Timer Flag	2-14-50
2-15.3.14	Transaction Counter	2-14-50

This page is intentionally left blank

2-2 Revision Log, Book 2

This revision log concerns only changes to book 2 and only changes after release of version 3.0 are included.

See also chapter 1-2, Revision Log, Book 1

Version	Date	Last Page	Affects	Brief Description of Change
3.1.2	2010-03-25	Book 2	Chapter 4	The whole text in section 2-4.15 is rewritten to highlight the requirements for fallback to magnetic stripe from ICC. The functional requirements are unchanged.
3.2.0	2010-06-15	Book 2	Chapter 3	Add that Norwegian terminals shall support Track3. Clarify key description.
3.2.0	2010-12-20	Book 2	Chapter 4	Add reference to new Visa standard. Update cross reference table on transactions in section 2-4.2. Add info on relaxed guard time in section 2-4.6. Add info on track3 requirements in section 2-4.7. Add info on handling of Cancellation and Post transactions in section 2-4.8. Update section 2-4.17 on fallback.
3.2.0	2010-12-20	Book 2	Chapter 5	In section 2-5.3 clarify that this is a generic requirement. In section 2-5.4 add note on handling of Cashback. A new section <deprecated> defining the requirements for PSAM based terminals is added. During Start-Up, a new Get Debit/Credit Properties (Identifier = '0009'), replacing the old Get Debit/Credit Properties (Identifier = '0001') is introduced. Add information in section 2-5.11 on Cancellation. Add section 2-5.11 on Post Registration. Add information on handling of Prepaid MSC transactions in section 2-5.15. Clarify use of Authorization Advice in section 2-5.16. Update table 2-5.6 to use English as language. Add Fig. 2-5.40 on extracting Update Commands.
3.2.0	2010-12-20	Book2	Chapter 9	Add information on Preferred Offline.
3.2.0	2010-12-20	Book2	Chapter 12	Rewrite of to reflect a new way of handling Private Label Card schemes.
3.2.0	2010-06-15	Book 2	Chapter 13	Messages for handling of (Norwegian) Reconciliation added. Add Field 4 and Field 54 in Authorization Request Response. Add Field 36, Track3 data, for MSC transactions. Add Tables with commands for ICC Prepaid cards. Add Field 44 in the Request response from the host. Add information on change of Field 44, Acquirer information and PSAM version. Add information on change of Field 46, new PSAM version. Add information on change of field 47 with Offline transaction (in Norway). Prepaid APACS messages are added and a description of field 54 (Amounts, additional) is inserted. Add information on AID and Expiry date included in Field 55. Add information on transfer of Reconciliation Report data in Field 63. Add POS Capability Codes for Post Registration.

3.2.0	2010-06-15	Book 2	Chapter 14	<p>Command for handling of Cancellation added. Add command Submit Card Reference 2, used for Extended Authorization TR=09.</p> <p>A new set of contactless commands is introduced (Initiate Contactless Payment, Contactless Payment, Validate Data 2 and Complete Payment). A new Get Debit/Credit Properties (Identifier = '0009'), replacing the old Get Debit/Credit Properties (Identifier = '0001') is added.</p> <p>Get Debit/Credit Properties with Identifier = '0002' is extended to handle Track3 cards.</p> <p>Get Debit/Credit Properties with Identifier = '0009' to '000E' added.</p> <p>Set Debit/Credit Properties extended with the possibility of setting Selectable Kernel Configurations. PSAM update extended with Firmware update.</p> <p>The response to the Validate Data 2 command is extended to deliver amount related to Prepaid ICC transactions under certain conditions.</p> <p>Update Get Amount 3 to specify the special Track3 data format.</p> <p>Add ASW's for Patch Update handling.</p> <p>Add ASW for more detailed TVR/IAC declined handling.</p> <p>Add ASW's for Private Label Card schemes.</p> <p>Add ASW for handling of Alternate Kernel Configuration capabilities</p> <p>New data elements related to Prepaid ICC are added.</p>
3.2.0	2010-06-15	Book 2	Chapter 15	<p>Multiple new data elements for Prepaid ICC (Contactless) added. New data elements related to Dual Kernel Configuration added. Update specification for Card Reference. Add information for Private Label Card Scheme in Card Service Info. Add Dual Card Reference. Update Merchant Initiative to handle Dual Kernel Configuration and Preferred Online. Add Track3 Data, Update specification for Transaction Request. Add Post Purchase/Refund to Transaction Request.</p>
3.3.0	2011-10-15	Book 2	Chapter 4	<p>Card Data Protection (CDP) has been introduced in section 2-4.15.</p>
3.3.0	2011-07-21	Book 2	Chapter 4	<p>Section 4.2.7 clarify use of MSC reader. Section 4.15 clarify rules for handling of fallback.</p>
3.3.0	2011-10-15	Book 2	Chapter 5	<p>Card Data Protection (CDP) has been introduced.</p>
3.3.0	2011-07-21	Book2	Chapter 5	<p>Emphasize that transaction flow is based on ASW1 ASW2 only. Add D/C Properties to fig. 2-5-1. Section 5.16 Change naming of files. Rework handling of File 5, remove locking of terminal.</p>
3.3.0	2011-07-21	Book2	Chapter 13	<p>Table 2-13.125 Add values for Post registration. Introduce Field 59 and add description of format of Extended Issuer Envelope (Field 59).</p>
3.3.0	2011-04-21	Books	Chapter 14	<p>Add MT's '47' and '48' to table 2-14-1. Section 2-14.5 update Get D/C prop. and Set D/C prop. with handling of encrypted card data and Extended Issuer Envelope. Section 2-14.6 Update commands and data formats taking Card Data Protection into account. Section 2-14.9 add Card</p>

				Data Protection, CDP, commands. Section 2-14.10 update ASW's to take CDP into account.
3.3.0.	2011-07-21	Book2	Chapter 15	Add data definitions for [Card Data], Extended Issuer Envelope, Mode, PIN block format, Seed and [Track Data]. Extend definitions for Issuer Envelope, PAN and Terminal Settings.
3.3.0	2011-08-18	Book2	Chapter 2 a.s.o.	Use concept of "Secure Device" instead of "Tamper Evident Device"
3.3.0	2011-08-18	Book2	Chapter 14	Update Terminal Settings
3.3.0	2011-10-15	Book2	Chapter 4	Remove section 2-4.7.5 Interface to Processor Card Interface. Update section 2-4.10 PSAM handler.
3.3.1	2012-02-20	Book2	Chapter 5	Update table 2-5.1 to include log activation and log recording.
3.3.1	2012-02-20	Book2	Chapter 13	Add additional Tags to table 2-13.-143 in Extended Issuer Envelope
3.3.1	2012-02-20	Book2	Chapter 14	Update section 2-14.4.3 to support returning only Private Label BIN ranges. Update section 2-14.5.6 to support identifier '00016' returning security configuration. Update section 2-14.5.9 to support the return of log information. Change section 2-14.10.1 to block displaying Card Blocked on Cardholder display.
3.3.1	2012-02-20	Book 2	Chapter 15	Add term PSAM Security Configuration. Update Terminal Settings to handle login enable/disable bit.
3.3.2	2012-12-01	Book2	Chapter 4	Section 2-4.7.2, clarify requirement of non card conflict. Section 4.16.3, specify fallback to contact for contactless cards.
3.3.2	2012-12-01	Book2	Chapter 5	Section 2-5.1.2, update Fig. 2-5.1, 2-5.2 and 2-5.3 to reflect the flow at contactless terminals.
3.3.2	2012-12-01	Book2	Chapter 13	Section 2-13.8 add note that message formats include contactless transactions as well. Section 2-13.9.1, add field 59 handling. Section 2-13.9.5, add proximity payment / consumer device. Update table on POS capability and POS entry mode. Extend Table 2-13.99 to handle new Action code from host. Extend Table 2-13.106 to handle Contactless specific data elements. Update Table 2-13.109 with new tag for Customer Reference Number.
3.3.2	2012-12-01	Book2	Chapter 14	Section 2-14.4.3 add new identifiers for Get D/C Properties to handle contactless cards. Section 2-14.6.4, update the Complete command to handle Transaction Status. Section 2-14.6.16 Add the Initiate Contactless Payment command. Section 2-14.6.17 add the Validate Contactless command. Section 2-14.6.18 add the Complete Contactless Command. Table 2-14.127 add new ASW's related to contactless transactions here and in other ASW tables.. Table 2-14.129 add ASW to detect Key _{CDP} missing. Table 2-14.136 add ASW's for contactless / loyalty cards.

3.3.2	2012-12-01	Book2	Chapter 15	Section 2-15.2, add / update following data elements: - Action Indicator, Approval code, AOSA, Card Data Source, Contactless Terminal Settings, CVM Status, Default Kernel ID, Dual Card Reference, Error code, Kernel ID, Limit Info, Magstripe Indicator, PSAM Security Configuration, Settings _{CL} , Terminal Settings, Transaction Identifier, Transaction Status,
3.3.3	2013-01-15	Book2	Chapter 14	Section 2-14.5.8 add function Get Random Number. Section 2-14.6.26 and 2-14.6.27 add function Retrieve Card Data
3.3.3	2013-01-15	Book2	Chapter 15	Section 2-15.2.29 update Card Service Info, 2-15.2.51 update Dual Card Reference. Section 2-15.2.113 add RandomNumber. Section 2-15.144 to 2.15.146 update information on MSC track data.
3.3.3	2013-01-20	Book2	Multiple	Make reference to EMV specification version independent.
3.3.3	2013-04-23	Book2	Chapter 6	Make req. 2-6.1.3.1 - 2-6.1.3.3 and 2-6.1.3.12 B requirements.
3.3.3	2013-04-23	Book2	Chapter 6	Requirement 2-6.4.2.4 concerning EMV rules for the checksum is added.
3.3.3	2013-05-02	Book2	Chapter 13	Add four additional Tags to Field 55 definitions. table 2-13.108. Add four additional Tags to field 69 (6J, 6K, 6R and UQ) definitions, table 2-13.111.
3.3.3	2013-05-13	Book2	Chapter 13/14	Change maximum length of the Issuer Envelope Data for EMV from 150 bytes to 100 bytes.
3.3.3	2013-06-17	Book2	Chapter 15	Update specification for Card Data (CV-2)
3.3.4	2013-08-20	Book 2	Chapter 14	2-14.5.8 Add Retrieve Hash Value in Get D/C Properties. 2-14.6.16 Correct errors in Initiate Contactless Payment.
3.3.4	2013-08-28	Book 2	Chapter 15	Add definitions Algorithm Id, Salt, Salt version, Scheme Id, Scheme Id Bitmap and Transaction Options. Update PSAM security configuration.
3.3.4	2013-10-03	Book2	Chapter 5	2-5.1 Add information on new PTS key synchronization (Install2). 2-5.2 Update conditional use of CheckStopList. 2-5.12 Include Install2 in flow.
3.3.4	2013-10-03	Book2	Chapter 13	2-13.8 New network Management Request and Response format due to PTS. 2-13.9 New field 46 parameters.
3.3.4	2013-10-03	Book2	Chapter 14	2-14.5 New PTS related commands, GetKey-CheckValue 2, Submit Initial Key 2, Initiate PIN 2 and Install 2. New get D/C properties for Surrogat PAN. 2-14.6 Add TO for Contactless. 2-14-10 a couple of new ASW's.
3.3.4	2013-10-03	Book2	Chapter 15	2-15.2 Add new data elements related to PTS and electronic Receipts.

2-3 System Overview

2-3.1 Terminal Model

2-3.1.1 Terminal Architecture for PSAM Applications (TAPA)

This section briefly describes the structural components comprising the Terminal Architecture for PSAM Applications (TAPA) as depicted in figure 2-3.1.

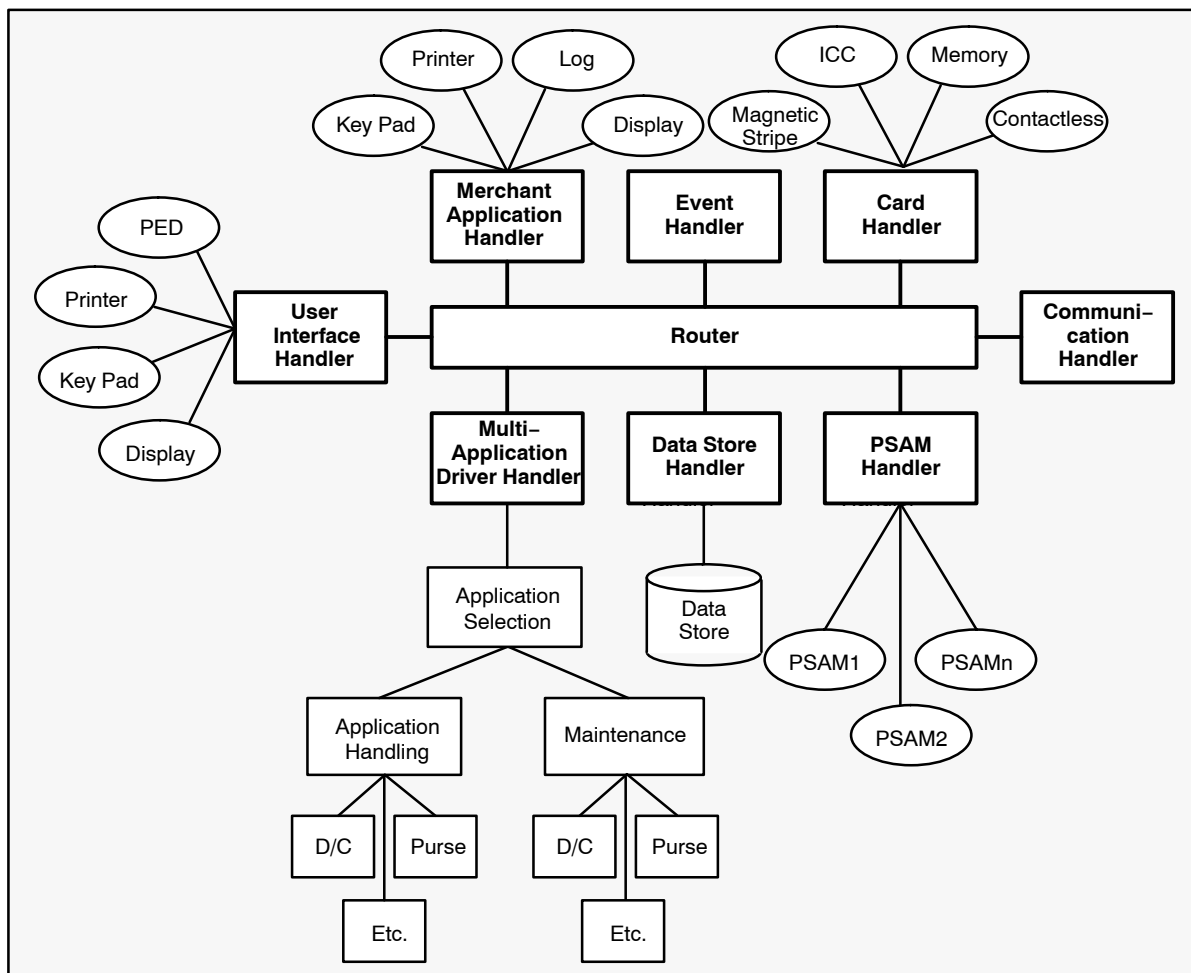


Figure 2-3.1 - Terminal Architecture for PSAM Applications (TAPA)

The components of this terminal architecture are the router, the various device handlers and the multi-application driver handler (MAD-Handler). One or more PSAMs are used.

The Router

The Router forms the central communication channel between the handlers in the terminal. It must be built as a pure transport mechanism and, consequently, be completely application independent.

The Handlers

The handlers form the standardized interfaces to the physical devices. An application only needs to know the interface to a certain handler to be able to communicate with a given device.

It is strongly recommended that handlers be application independent wherever possible.

The Multi-Application Driver Handler (MAD-Handler)

The MAD-Handler is the software in the terminal that actually drives the terminal. It will always be present to some degree.

The total functionality for a given application is shared between the MAD-Handler and the corresponding PSAM. In some implementations based on TAPA, the PSAM will only perform cryptographic functions whereas the implementation defined in this specification leaves much of the application functionality to the Nets PSAM.

Requirements to the debit/credit application are all defined in detail in this specification.

The PSAMs

In this implementation, terminal control is handed over to the PSAM by the MAD-Handler for all card related communication (except for application selection).

Furthermore, the PSAM builds all transaction related messages to be sent to the host systems.

This philosophy gives a high degree of flexibility on the overall terminal behavior just by updating parameters in the PSAM. Larger changes can be handled by software updates in the PSAM or by physically changing the PSAM to a newer version. In any of these cases, the MAD-Handler software need not be modified.

The Nets PSAM is developed by Nets Denmark A/S as Terminal Operator.

2-3.2 A Physical Implementation of the TAPA Model

Figure 2-3.2 shows a physical implementation of the TAPA model where the handlers and devices have been grouped according to physical housing and interconnections.

Merchant related devices have been grouped in the Merchant Application, e.g. an electronic cash register or a back-office system. The PIN Entry Device (PED), chip card reader and cardholder display have been physically enclosed in the Secure Device, and except for the PSAMs, the remaining handlers and devices constitute what is called the CAD (Card Accepting Device).

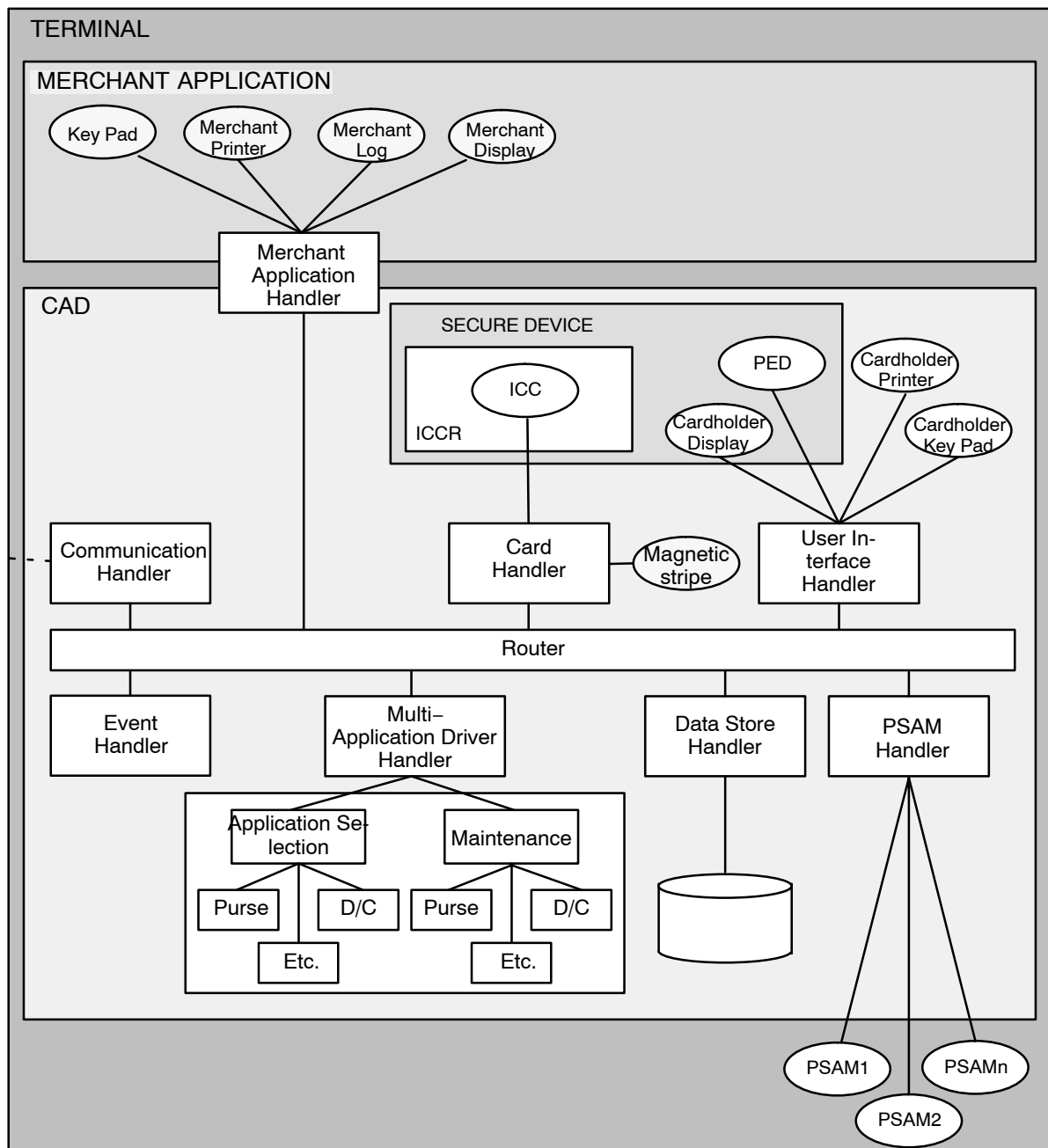


Figure 2-3.2 - Example of a Physical Implementation

2-3.2.1 Merchant Application

The Merchant Application contains all functionality not directly related to the payment application, e.g. in an electronic cash register, the price look-up and totalling.

In an unattended terminal, the user selects a certain service, and the Merchant Application transforms this into a request for a payment transaction handled by the MAD-Handler.

- 2-3.2.1.1 C The Merchant Application may have user interfaces of no direct relation to the payment functions such as signal lamps and activation keys or handles specific for the purpose of the terminal.

- 2-3.2.1.2 A If the terminal is attended, the Merchant Application shall contain a merchant display to guide the merchant.

2-3.2.2 The MAD-Handler

The terminal specified will be able to handle credit and debit cards. Debit and credit cards can be ICCs and/or MSCs (Magnetic Stripe Cards). Any transaction initiated with a MSC will - if possible - be performed online with the acquirer/issuer in order to authorize and settle the transaction and to validate the card and the PIN.

The ICC and the PIN can also be validated online. The ICC and the PIN can, however, be verified and validated offline if both card issuer and acquirer allow offline processing.

The MAD-Handler applications are the central elements/building blocks in the terminal generating and transmitting all possible types of transactions, including administrative transactions, to the acquirer/issuer directly or via a Terminal Operator. It is the MAD-Handler applications that control the transaction flows in online operations as well as in offline operations.

2-3.2.3 Card Readers (General)

The card readers for magnetic stripe cards and chip cards should preferably be combined but can be separate if required by the terminal design:

- manual swipe reader for magnetic stripe cards
- manual insertion reader for chip cards (and possibly also magnetic stripe cards)
- motorized reader for both chip cards and magnetic stripe cards

- 2-3.2.3.1 A Unattended terminals shall have a combined card reader.
- 2-3.2.3.2 C If the card reader is motorized, the card may be retained in the terminal at the card issuer's request.

2-3.2.4 Magnetic Stripe Card Reader

- 2-3.2.4.1 A The magnetic stripe card reader (MSCR) shall as a minimum be capable of reading the ISO-defined track 2 of the magnetic stripe.
- 2-3.2.4.2 C Terminals may as well be capable of reading track 1 and track 3 of the magnetic stripe.

2-3.2.5 Integrated Circuit Card Reader

The ICC Reader (ICCR) can be designed as either a manually operated reader or a motorized reader.

- 2-3.2.5.1 A If the ICCR is not integrated with the PED, it shall be housed in an Interface Device.
- 2-3.2.5.2 A The Interface Device shall be a Secure Device with cryptographic functions.

- 2-3.2.5.3 A The ICCR shall be capable of resetting and communicating with ICCs according to the requirements in ref. 20: "EMV ICC Specification".

2-3.2.6 PIN Entry Device (PED)

The PED is a Secure Device used to enter the PIN. The PIN is enciphered and sent to the PSAM which either sends it on-line to the issuer or lets the ICC itself validate the PIN offline. In both cases, the PIN is re-enciphered before transmission from the PSAM.

See section 2-6.2.8 page 2-6-6 and chapter 2-6 in general. Regarding privacy shield, see chapter 2-7.

2-3.2.7 Displays

The main purposes of the cardholder display are to provide the cardholder with user guidance, e.g. for application selection, and transaction related information.

Standardized text strings allow the same cardholder dialog in terminals from different Terminal Suppliers.

- 2-3.2.7.1 C For attended terminals, a merchant display may give user guidance to the merchant and allow him to follow the transaction progress.

The transaction result is shown in both display types.

2-3.2.8 Receipt Printer

- 2-3.2.8.1 A For debit/credit transactions, the cardholder shall, as default, always be able to get a receipt with relevant transaction information printed, including the result of the transaction.
- 2-3.2.8.2 A For each transaction initiated, a receipt shall be printed, even if the transaction was rejected or failed.
- 2-3.2.8.3 A When using a UPT terminal, the cardholder shall have the option to select a receipt.
- 2-3.2.8.4 A If a receipt cannot be printed, e.g. the printer is out of paper, the cardholder shall be notified before being requested to accept the transaction amount.

2-3.2.9 Command Keys

The main purpose of the command keys is to enable the cardholder to interact with the terminal.

- 2-3.2.9.1 A At least two keys shall be implemented: ENTER and CANCEL.
- 2-3.2.9.2 C A CLEAR key may also be implemented.
- 2-3.2.9.3 C The three keys, ENTER, CANCEL and CLEAR, may be contained in the PIN Pad or other secure environment.

- 2-3.2.9.4 A If, on an unattended payment terminal, the cardholder keyboard contains numeric keys, it shall be very clear to the cardholder what is the PIN Pad and what is the cardholder keyboard.

This is in order to ensure that the cardholder enters the PIN on the PIN Pad and not the cardholder keyboard with the risk of disclosing the PIN.

2-3.2.10 Data Store

Transaction data created by the PSAM for debit/credit card transactions is stored in the Data Store. The MAD-Handler can also use the Data Store for its own purposes.

2-3.2.11 Logging Devices

If a dedicated log device exists in the Merchant Application, the PSAM will, in addition to the transactions stored in the Data Store, be able to send the most vital transactions for back-up storage in such a log device. Data originating from the PSAM will only be used in case of Data Store errors.

The MAD-Handler and/or the Merchant Application can also use the log device for their own purposes.

The log device can be designed as a printer unit or data can be stored electronically, e.g. on a disk or another kind of non-volatile memory.

2-3.2.12 Transfer of Stored Debit/Credit Transactions

Debit/credit transaction data stored in the terminal as the result of offline transactions will be sent to the Terminal Operator as described in section 2-5.15. This transfer can continue until there are no more messages to be sent.

The Terminal Operator will acknowledge each message received.

2-3.2.13 The Interface(s) to the PSAM(s) and the PSAM functions

The PSAMs contain application related security functions and parameters as determined in the merchant-Terminal Operator/acquirer agreements.

During terminal initialization, the PSAMs will send configuration parameters, e.g. card selection tables, to the MAD-Handler for use in the application selection process.

The Nets PSAM create the transactions and perform the security analysis of the responses received from the Nets Denmark host system.

The Nets PSAM is maintained centrally by having certificates, encipherment keys and new configuration parameters sent from the Terminal Operator in update messages.

The PSAM is capable of performing both Static Data Authentication (SDA), Dynamic Data Authentication (DDA) and Combined DDA/AC Generation (CDA) verifications for EMV

debit/credit cards and holds the necessary Certification Authority (CA) Public Keys for the card schemes for which Nets Denmark is the acting acquirer.

The PSAMs will synchronize with the PED, such that the PED and the PSAMs will be able to communicate secretly, i.e. using encrypted messages. After synchronization, the PED will be able to encrypt an online PIN for transmission to the selected PSAM and an offline PIN for transmission to the ICC.

In the Nets PSAM, the online PIN will be decrypted and re-encrypted using a dedicated online PIN encryption key. The offline PIN can be sent to the ICC in plaintext, depending on the ICC. In any circumstance, the offline PIN, encrypted or plaintext, will be sent from the PED to the ICC via the Nets PSAM.

The PSAM will contain the necessary keys for encrypting online and offline messages.

The PSAM will store the public keys necessary to validate certificates read from ICCs.

2-3.3 Application Selection

The basic application selection principle in the terminal is based upon the input from a handler in the terminal.

As depicted in figure 2-3.3, input to the MAD-Handler application selection can come as either a business call from the Merchant Application or as a 'card inserted' event from the card handler. In most cases, information from both sources are required in order to determine which function to perform.

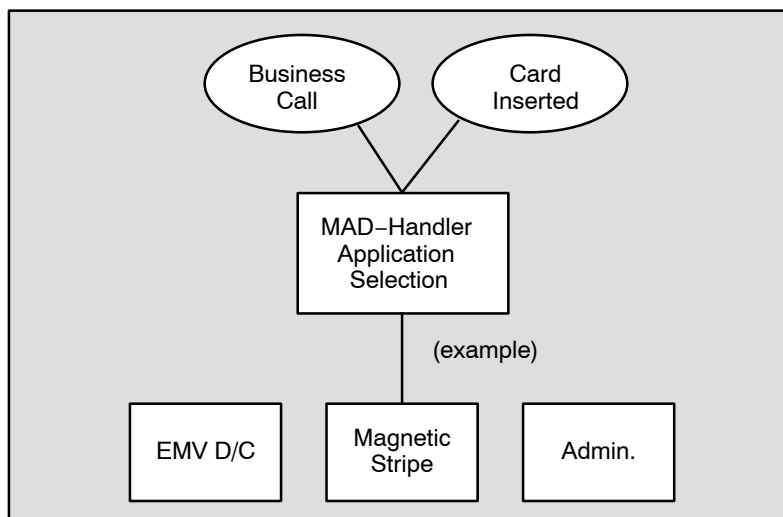


Figure 2-3.3 - Application Selection Principle (Example)

One of the main functions in the terminal is the application selection mechanism. The application selection must ensure that the card read in either the MSCR or the ICCR will result in selection of the correct application. Dialog with the cardholder can be necessary.

The terminal will know which applications are supported by referring to information installed by the Terminal Supplier (or Terminal Operator). Card selection data will be read out of each PSAM and stored in the terminal at initialization time for usage whenever a card is read. For MSCs, the application selection will be determined from a table of PAN prefixes, and for ICCs, the selection process will be based on a table of AIDs.

2-3.4 Security Zones, Debit/Credit

The terminal being specified is seen as a basic element in the infrastructure for card transactions in which Nets Denmark A/S takes part. Consequently, the security requirements are those fulfilling the security level required by Nets Denmark A/S and its cooperating partners.

The PIN Entry Device (PED) or PIN Pad and the Nets PSAM creates a security zone from which it will not be possible to retrieve an entered PIN in plaintext. From other applications - if not using a PSAM - it will be possible to send a reference PIN or a PIN verification value to the PED. This facility will, in a secure way, enable the PED to compare/verify the entered PIN and forward the result to the MAD-Handler.

The TAPA architecture makes it technically possible to pass transactions to various Terminal Operators. The handling of an online PIN is secured within the security zone between the PED and the PSAM active for the selected terminal application. Each application and corresponding PSAM need to establish their security zone with the PED before a PIN may be transferred. Mutual recognition of the PSAMs is necessary in order to ensure the secrecy of the PIN for all applications.

When initializing the terminal, security zones are established between the PSAMs and the PED. Hereafter, PINs can securely be transmitted between the PED and the selected PSAM.

As depicted in figure 2-3.4, one PSAM (PSAM 1) is controlling the security zones between the PSAM and the PED, PSAM and ICC Reader and between the PSAM and the Terminal Operator. The PSAM receives the enciphered PIN from the PED and creates the PIN block to be transmitted to the Terminal Operator. This security mechanism ensures the protection of the online PIN as the PIN is always transmitted in an enciphered form.

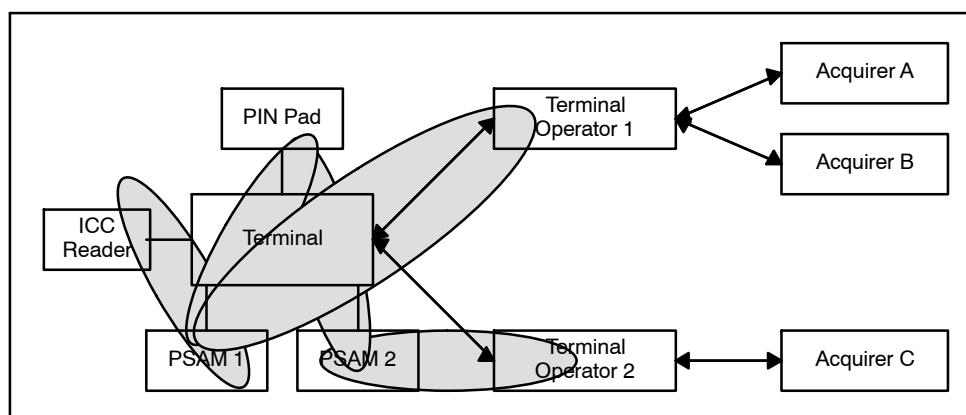


Figure 2-3.4 - Security Zones in an Open Terminal Environment

When another application needs to have a PIN validated, the PSAM (PSAM 2) does not and cannot use security zone 1 because of the possibility of having the PIN sent to the wrong Terminal Operator together with information from the chip or the magnetic stripe.

A second security zone exists between the PSAM and the Terminal Operator issuing the PSAM and the PSAM encipherment keys.

For EMV cards supporting Dynamic Data Authentication (DDA/CDA), a third security zone exists between the PSAM and the EMV card.

The terminal must as a minimum provide tamper evidence to the following elements: the ICCR, the PIN Pad and the Cardholder Display.

The PIN Pad itself shall be tamper responsive, i.e. capable of erasing all useful information and encipherment keys when detecting an attack.

2-4 General Requirements

2-4.1 Introduction

This chapter contains requirements that are common to all terminal applications, irrespective of the card types accepted.

2-4.1.1 Related Specifications

When requirements in this specification overlaps requirements in the referenced specifications, this specification has precedence.

Terminal Specifications

The terminal is based upon the architecture described in ref. 27: "TAPA, Application Architecture Specification".

- 2-4.1.1.1 A Except when specifically stated, the terminal shall comply with ref. 27: "TAPA, Application Architecture Specification".

NOTE: This common architecture allows implementation on top of existing terminal architectures such as OTA, OPT, ITA, STIP, etc.

- 2-4.1.1.2 A The terminal shall comply with ref. 20: "EMV ICC Specification" and related bulletins issued by EMVCo.

NOTE: As EMV is "non-forgiving" and "non-waivered", all mandatory terminal related requirements in ref. 20: "EMV ICC Specification" shall be met.

NOTE: EMVCo bulletins are designed to keep financial institutions, vendors, and other interested parties, informed of any important enhancements relating to the EMV specifications, their implementation and approval processes.

- 2-4.1.1.3 A Furthermore, the terminal shall comply with the terminal specifications as issued by card schemes, e.g. ref. 29: "Visa Transaction Acceptance Device Requirements" and ref. 31: "Terminal Requirements for Acceptance of Chip Pay Now (Debit) and Pay Later (Credit) Cards".

NOTE: The card schemes define requirements for optional features in the EMV specification which then becomes mandatory. These specifications can be obtained from the card schemes' websites given in section 1-4.6, "Related Websites".

2-4.2 Card Related Transactions

2-4.2.1 Transaction flow

Table 2-4.1 gives a cross reference to the transaction flow figures applicable for specific combinations of Business Calls and sources of transaction data.

Table 2-4.1 - Transaction flow figures vs. Business Calls and Sources of Transaction Data

	Purchase	Original Authorization	Extended Authorization	Supplementary Auth.	Capture
EMV					
PIN	Figure 2-5.6	Figure 2-5.9	Figure 2-5.9 & 2-5.10	-	-
Signature	Figure 2-5.7	-	-	-	-
No CVM	Figure 2-5.8	Figure 2-5.9	Figure 2-5.9 & 2-5.10	-	-
MSC					
PIN	Figure 2-5.13	Figure 2-5.16	Figure 2-5.16	-	-
Signature	Figure 2-5.14	-	-	-	-
No CVM	Figure 2-5.15	Figure 2-5.17	-	-	-
Key Entered					
PIN	-	-	-	-	-
Signature	Figure 2-5.20	-	-	-	-
No CVM	Figure 2-5.21	Figure 2-5.22	-	-	-
Token					
PIN	-	-	-	-	-
Signature	-	-	-	-	Figure 2-5.25
No CVM	-	-	-	Figure 2-5.24	Figure 2-5.26
Refund					
	Refund	Reversal	Cancellation		
EMV					
PIN	-	-	-		
Signature	Figure 2-5.11	-	-		
No CVM	-	-	Figure 2-5.12		
MSC					
PIN	-	-	-		
Signature	Figure 2-5.14	-	-		
No CVM	-	-	Figure 2-5.19		
Key Entered					
PIN	-	-	-		
Signature	Figure 2-5.20	-	-		
No CVM	Figure 2-5.21	-	Figure 2-5.23		
Token					
PIN	-	-	-		
Signature	-	-	-		
No CVM	-	Figure 2-5.27	-		
Legend:					
Figure 2-5.X refer to the figure showing the transaction flow for the transaction in question.					
- indicates that the transaction is not applicable.					

2-4.2.2 Cancellation

TAPA Commands

Terminals able to handle Cancellation must support the following TAPA commands:

- Get File Record
- Delete File record

These commands are issued by the PSAM during the Cancellation transaction. The *Get File Record* command is used to check if the previously created Financial Advice still is present and valid. The *Delete File Record* command is used to delete the previously created Financial Advice, when all the conditions for performing a Cancellation transaction is fulfilled.

Message Reason Code

It is possible to distinguish a Reversal Advice created as part of Cancellation transaction by the value of the Message Reason Code (MRC). The value of 4005 (Original amount incorrect) indicates that a Cancellation transaction has been performed.

Merchant Log

If the Merchant Log is enabled, the Reversal Advice created during the Cancellation transaction will be stored at the Data Store and the Merchant Log respectively.

2-4.3 Tokens

2-4.3.1 Format and Retrieval of the Token

The Token consist of two parts, a header denoted the "Info field" containing the necessary information for the merchant to perform Token based transactions. The second part contains Token data which includes enciphered transaction data, a digital signature and public key certificate(s).

Token data are enciphered when sent to and from the PSAM.

As the Token can be generated and interpreted by a PSAM only, the format and contents of the enciphered part are considered proprietary.

- 2-4.3.1.1 A The terminal shall be able to handle Tokens with a total length of up to 1024 bytes.

The format of the Token can be found in table 2-4.2.

Table 2-4.2 - Format of the Token

	Field	Description	Length
I N F O	Token Format	Either 'D2' (EMV), 'D4' (MSC track 2) 'D6' (Key Entered) or 'D8' (MSC track 3)	1
	Token version	Binary version number (Initial value: '01')	1
	LEN _{AID} + AID/Pre-fix	LEN _{AID} + AID with trailing zeroes or first 6 digits of the PAN padded with 'FF'	17/4
	Accumulated amount	Accumulated amount (binary) of each authorization	4
	CURRC	Currency Code	2
	CURRE	Currency Exponent	1
	VK _{CA, TOKEN}	Key version of the PK _{CA, TOKEN} used to verify the Token Public Key Certificate (PKC _{PSAM, TOKEN})	1
	VK _{TOKEN}	Key version of the CK _{TOKEN} key used to encipher the Token Transaction Data	1
	ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported	1
	Merchant Number	Used by the merchant to verify whether a Token created in another shop is valid in the actual shop	5
	LEN _{A+B}	Variable used by the PSAM when deciphering the field "Token Data" (LEN _{A+B} does <i>not</i> specify the length of the field "Token Data")	2
	Token Data	Token Transaction Data enciphered and signed	
Total			Up to 1024
NOTE: The first 23/36 bytes (denoted "INFO") are all in plaintext in order to provide the merchant with the necessary data to handle Tokens, while the actual Token Transaction Data (the grey row) are enciphered and signed. Plaintext data are protected against modification by use of a hash function.			

2-4.3.2 The use of Tokens

A number of terminal specific requirements concerning the use of Tokens are defined.

- 2-4.3.2.1 A When initiating a Reversal (Authorization), the amount fields in the *Initiate Token Based Payment* command shall be omitted, i.e. that LEN_{AMOUNTS} = '00'.
- 2-4.3.2.2 A The Merchant Initiative (MI) shall be set to '00' when performing a token based transaction. The value '00' means that neither a online/offline transaction nor a specific CVM are forced by the merchant.
- 2-4.3.2.3 A Tokens shall be stored (logically) in the Merchant Application.

2-4.4 Cardholder Verification

2-4.4.1 PIN Entry

See section 1-14.7

2-4.4.2 Signature

Signature Verification Function

- 2-4.4.2.1 A If the Signature Verification function is required by the PSAM (indicated in the response to the *Exchange Debit/Credit Static Information* command), the MAD-Handler shall request the merchant to decide whether the cardholder's signature just written on the receipt compares to the reference signature on the Card.

NOTE: Only the PSAM is able to enable/disable the Signature Verification function as used by the PSAM.

- 2-4.4.2.2 A The *Verify Signature* command shall be used to request the merchant for signature verification.

- 2-4.4.2.3 A If the Signature Verification function is enabled, the transaction shall only be completed successfully if the merchant responds positively by pressing a "Yes/OK" function key to the question: "Signature OK?"

- 2-4.4.2.4 A If the Signature Verification function is enabled, but the merchant does not respond positively to the question "Signature OK?", then the transaction shall be voided.

NOTE: The PSAM controls this void function.

- 2-4.4.2.5 C The terminal may use the signature verification function even if the PSAM does not require Signature Verification as indicated in the response to the *Exchange Debit/Credit Static Information* command.

NOTE: The PSAM reacts to the Transaction Status ('01'/'81') in the *Complete Payment* command and controls the void function even if the PSAM did not require Signature Verification itself.

2-4.5 The Router

The Router controls all communication between the individual handlers in the terminal.

2-4.5.1 Functional Requirements

- 2-4.5.1.1 A The Router shall conform to the requirements in ref. 27: "TAPA, Application Architecture Specification", section 4.1.

2-4.5.2 Command Flow

The command flow is defined in ref. 27: "TAPA, Application Architecture Specification", section 4.2.

2-4.6 Multi-Application Driver Handler (MAD-Handler)

2-4.6.1 General Requirements

- 2-4.6.1.1 A The MAD-Handler shall perform the start-up sequences for all terminal applications and related PSAMs before allowing the initiation of a transaction in any terminal application.
- 2-4.6.1.2 A The MAD-Handler shall finish the start-up sequence for one terminal application before starting the next.
- 2-4.6.1.3 A The MAD-Handler shall keep track of the current cardholder dialog, e.g. by implementing a state machine.

Clean Up and Guard Time

In order to minimize the processing time in the PSAM, the PSAM will perform some processing (clean up) after the response to *Complete Payment* has been returned to the terminal.

During this processing (clean up), the PSAM is not able to receive a new command. Any command sent to the PSAM immediately after the response to an approved *Complete Payment* command is received, may not be understood by the PSAM.

The *Complete Payment* command is the only command that may cause extensive processing inside the PSAM, after the response has been sent.

- 2-4.6.1.4 A After the response to an approved *Complete Payment* command is received, a delay of minimum 500 milliseconds shall elapse, before any new command shall be sent to the PSAM.

NOTE: No delay is needed after *Complete Payment* in a declined transaction.

NOTE: Processing in the terminal, not involving the PSAM, shall not be influenced by this guard time.

2-4.7 Card Handler

2-4.7.1 General Requirements

- 2-4.7.1.1 A If the debit/credit application described in this specification is implemented, the following sub-handlers shall be implemented:
- Processor card reader
 - Magnetic stripe reader

Card Selection

- 2-4.7.1.2 A Technology selection, i.e. IC, contactless IC or magnetic stripe, shall be done in accordance with ref. 20: "EMV ICC Specification".
- 2-4.7.1.3 A A combined card reader shall attempt to read the IC first. If this fails, the magnetic stripe shall be read.

NOTE: The above requirement is as seen from the outside world. Depending on the technology used, the magnetic stripe may physically have been read when the card was inserted.

When the terminal has determined the card technology, the application selection process can start.

2-4.7.2 Magnetic Stripe Card Reader (MSCR)

Conformance to TAPA

- 2-4.7.2.1 A The MSCR shall conform to ref. 27: "TAPA, Application Architecture Specification", section 6.1 with the following exceptions:
- Reading ISO track 1 is optional
 - Reading ISO track 3 is optional for some regions, see section 1-15 for detailed requirements.

Reading of ISO Track 2 and Track 3

NOTE: Design requirements related to the MSCR are defined in section 2-6.2.4.

Validation of ISO Track 2 and Track 3.

The task of the MSCR is to validate the characters read to identify reading errors. Validation of the contents of track 2 and track 3 is left for the MAD-Handler which also selects the proper PSAM and PSAM application to handle the transaction.

- 2-4.7.2.2 A The MSCR shall validate that all characters read have odd parity (the number of 1-bits read in the 5 (1+4) bits "P", "b4".."b1" shall be odd).

NOTE: This validation may either be performed "on-the-fly" or when the entire track has been read.

- 2-4.7.2.3 A The MSCR shall validate that the first character is a start sentinel (B'1011).
- 2-4.7.2.4 A The MSCR shall validate that the second last character is an end sentinel (B'1111).
- 2-4.7.2.5 A The MSCR shall assume that the last character is an LRC (longitudinal redundancy check) value and shall validate its value as defined in ref. 4: "ISO/IEC 7811-2", subclause 12.2.
- 2-4.7.2.6 A The MSCR shall validate that a maximum of 40 data characters are read from track 2 and, if supported, a maximum of 107 data characters are read from track 3 (including the start and end sentinels, the control characters and the longitudinal redundancy check character).
- 2-4.7.2.7 C The MSCR may be able to buffer up to 40 characters read from track 2 and, if track3 is supported, up to 107 characters read from track 3 (the entire track).
- 2-4.7.2.8 A The MSCR shall, when only track 2 is supported, be able to buffer the 37 characters that may be requested from other handlers in the CAD. The MSCR shall, if supporting track 3, be able to buffer the 104 characters that may be requested from other handlers in the CAD. These characters constitute the entire track data with the exception of the start and end sentinels and the LRC character. These three characters shall not be discarded until they have been validated (possibly "on-the-fly").
- 2-4.7.2.9 A If none of the above defined validations fail, the MAD-Handler shall be informed by posting an event indicating that a magnetic stripe card has successfully been read.
- NOTE:** The PSAM will perform any validation of the check digit in the PAN (Luhn-digit) and this check shall therefore not be considered as one of the validations mentioned above.
- 2-4.7.2.10 A If any of the above defined validations fail, the MSCR shall post an event to the Event Handler. Error information shall either be included in the (proprietary) Event Type Code, ref. 27 TAPA, or in the Response Code returned when the MAD-Handler issues the *Read Magnetic Stripe* command. This allows the MAD-Handler to display proper error messages to the cardholder and merchant.
- 2-4.7.2.11 B If a Card is swiped through the MSC reader or inserted into the ICC / Combined reader while a transaction is in progress, the terminal shall either not react to swiping the card or cancel the current transaction as long as the cardholder has not yet pressed the "ENTER" key.
- 2-4.7.2.12 A If the "CANCEL" key has been pressed and the card is retained in a motorized- or locking card reader, the card shall be returned immediately unless the cardholder has pressed the "ENTER" key.
- 2-4.7.2.13 C The terminal may, for specific regions, perform additional required validation of track 3. See section 1-15 for additional information.

- 2-4.7.2.14 A The terminal shall time out any pending (inactive) transaction after 45 seconds.

2-4.7.3 ICCR - General

- 2-4.7.3.1 A The ICCR shall comply with ref. 20: "EMV ICC Specification".

Repeat Last ICC Response

- 2-4.7.3.2 A Whenever the Card Handler responds to the *ICC Command*, the Card Handler shall store a copy of the three data elements from the response:
- L_{DATA}
 - Card Response
 - Response Code

- 2-4.7.3.3 A When the Card Handler receives a *Repeat Last ICC Response* command, the response shall contain the data elements previously stored (see requirement 2-4.7.3.2)

The format of the *Repeat Last ICC Response* command can be found in section 2-14.6.23.

2-4.7.4 ICCR - Processor Card Reader

General Requirements

- 2-4.7.4.1 A The Processor Card Reader shall always be aware, whether a Processor Card is present or not.
- 2-4.7.4.2 A If the Processor Card is not present, all commands received by the Processor Card Reader, but intended for the Processor Card, shall be rejected by the Processor Card Reader on behalf of the Processor Card using the proper Response Code.
- 2-4.7.4.3 A The Processor Card Reader shall always be aware, whether a proper communication has been established with the Processor Card.

NOTE: After a successfully completed ATR and possibly PPS, proper communication with the Processor Card has been established.

- 2-4.7.4.4 A If the Processor Card is present, but no proper communication has been established with the Processor Card, all commands received by the Processor Card Reader, but intended for the Processor Card, shall be rejected by the Processor Card Reader on the behalf of the Processor Card using the proper Response Code.

Commands to the Processor Card

- 2-4.7.4.5 A Command APDUs embedded in the *ICC Command* shall be routed transparently to the Processor Card and responses from the Processor Card shall be returned to the originator of the command APDU as defined in ref. 27: "TAPA Application Architecture Specification".

2-4.8 User Interface Handler

2-4.8.1 Cardholder Display

A number of “standard” display texts for guiding the cardholder are defined in table 1-11.1. Each display text is given a message identifier according to ref. 20: “EMV ICC Specification”.

General display requirements

- 2-4.8.1.1 A When the Currency Code is displayed, it shall be displayed in the corresponding alpha-characters according to ref. 12: “ISO/IEC 8859-15”.
- 2-4.8.1.2 A When the Confirm Amount commands is received a corresponding text derived from the Business Call (e.g. “Buy:” or “Refund:”), the Amount and the Currency Code (in alpha-characters) shall be displayed on the Cardholder Display and remain until the final transaction result is known.

NOTE: The text, amount and currency may remain at the Cardholder Display while the transaction result is displayed.

NOTE: The text, amount and currency may as well be displayed when cardholder confirmation is not requested.

NOTE: The text to be displayed are listed in table 2-4.4 (Business Calls Vs. Message Codes)

The commands sent from the PSAM to the User Interface Handler, when cardholder confirmation is requested, do not include information about the actual type of Business Call.

Therefore the information concerning the actual Business Call needs to be transferred to the User Interface Handler by other means.

E.g. the transfer (from the MAD-Handler to the User Interface Handler) may be based on the general *Write Handler String* command. The command may be sent from the MAD-Handler to the User Interface Handler just before the MAD-Handler is going to send the *Initiate Payment* command to the PSAM. If the PSAM subsequently requests services from the User Interface, the User Interface Handler will know the type of Business Call being processed.

Display Texts

The terminal needs to be able to convey appropriate display texts to both cardholder and merchant.

The physical requirements concerning the Cardholder Display can be found in section 2-6.2.5.

The display messages has a number (EMV message identifier) according to the standard messages defined in ref. 20: “EMV ICC Specification”.

Definition of Message Codes are assigned according to table 2-4.3.

Table 2-4.3 - Messages for Display and Printing

Message Code Range	
'01' – '3F'	Assigned by EMV
'40' – 'DF'	Assigned by TAPA
'E0' – 'FF'	Assigned by this specification

See section 1-11: "Localization: Display, Receipt Texts and Translations".

Display Requirements

During a transaction, the cardholder must be guided through a number of operational steps, e.g. PIN entry and amount confirmation.

The number of steps required depends on:

- the actual Business Call,
- the CVM selected (PIN, Signature, NoCVM or Combined),
- the PSAM configuration (PSAM Settings) concerning amount confirmation (configuration controlled from host-systems),
- the configuration of the terminal/PSAM (Info Level, bit b3). The coding of the data element can be found in table 2-15.13 on page 2-15-19.

The Message Code to be displayed at the Cardholder Display related to a specific Business Call can be found in table 2-4.4.

Additional requirements and examples can be found in section 1-11: "Localization: Display, Receipt Texts and Translations".

Table 2-4.4 - Business Calls Vs. Message Codes

Business Call	CVM Selected	PSAM Settings	Info Level bit b3	Message Code and Text	Comments
Purchase	PIN			'F0' "Buy:" 'EF' "PIN:"	PIN entry and amount confirmation
	Signature	0		'0E' "Wait"	No cardholder interaction
		1		'F0' "Buy:"	Amount confirm, only
	No CVM	0		'0E' "Wait"	No cardholder interaction
		1		'F0' "Buy:"	Amount confirm, only
Combined			'F0' "Buy:" 'EF' "PIN:"	PIN entry and amount confirmation	
Refund	PIN				Not applicable
	Signature	0		'0E' "Wait"	No cardholder interaction
		1		'86' "Refund:"	Amount confirm, only
	No CVM				Not applicable
	Combined				Not applicable
Original/ Extended Authorization	PIN		0	'EF' "PIN:"	PIN entry, only
			1	'F0' "Buy:" 'EF' "PIN:"	PIN entry and amount confirmation
	Signature			'0E' "Wait"	No cardholder interaction
	No CVM			'0E' "Wait"	No cardholder interaction
	Combined		0	'EF' "PIN:"	PIN entry, only
			1	'F0' "Buy:" 'EF' "PIN:"	PIN entry and amount confirmation
Supplementary Authorization	All			'0E' "Wait"	No cardholder interaction
Capture	All			'0E' "Wait"	No cardholder interaction
Reversal (Authorization)	All			'0E' "Wait"	No cardholder interaction
Cancellation	All			'0E' "Wait"	No cardholder interaction
Post Purchase	No CVM			'0E' "Wait"	No cardholder interaction
Post Refund	Signature			'0E' "Wait"	No cardholder interaction
<p>Legend: PSAM Settings (a PSAM data element) gives the acquirer the opportunity to request a confirmation of the amount. '1' denotes that confirmation of the amount is requested.</p> <p>"Combined" indicates the CVM consists of PIN & Signature.</p> <p>Grey cells means not applicable.</p>					

2-4.8.1.3

- B When the terminal is ready for a new customer, message codes 'E0' ("Terminal ready") or '0B' ("Insert Card") shall be displayed on the Cardholder Display.

- 2-4.8.1.4 B When an attended terminal is ready for a new customer but no receipt can be printed, Message Code 'E1' ("No receipt") shall be displayed on the Cardholder Display together with 'E0' ("Terminal ready") or '0B' ("Insert Card").
- 2-4.8.1.5 B If the terminal is out of order, message code 'EA' ("Out of order") shall be displayed on the Cardholder Display and no transactions shall be allowed.
- 2-4.8.1.6 B If the Log is out of order message code 'E8' ("Terminal failure") shall be displayed on the Cardholder Display and no transactions shall be allowed.
- 2-4.8.1.7 B If the terminal is busy, e.g. no vacant product outlets, message codes 'E9' ("Terminal busy") and '0E' ("Please Wait") shall be displayed on the Cardholder Display.
- 2-4.8.1.8 A When an unattended terminal is not able to print a receipt, the dialog with the cardholder shall give the opportunity (Yes/No) to proceed knowing that no receipt will be printed.
- 2-4.8.1.9 B When an unattended terminal is able to print a receipt, the dialog with the cardholder shall give the opportunity (Yes/No) to decide whether a receipt is desired. Message code 'E5' ("Receipt wanted?") shall be displayed on the Cardholder Display.
- 2-4.8.1.10 B When the terminal has attempted to read a MSC but a parity, LRC or format error has occurred, message code 'E3' ("Error reading card") and 'EE' ("Swipe/Insert card again") shall be displayed on the Cardholder Display.
- 2-4.8.1.11 C While the terminal performs application selection, message code '0E' ("Please Wait") may be displayed on the Cardholder Display.
- 2-4.8.1.12 B If the card was read successfully but not recognized, Message Code '0C' ("Not Accepted") shall be displayed on the Cardholder Display.
- 2-4.8.1.13 A The final transaction result based upon the ASW1-ASW2 value shall be displayed on the Cardholder Display.
- 2-4.8.1.14 A The Message Code '10' ("Remove Card") shall be displayed on the Cardholder Display when the transaction has been completed.
- NOTE:** This requirement is not relevant if the card does not remain in the card reader during the transaction.
- 2-4.8.1.15 B If the Message Code '10' ("Remove Card") cannot be displayed together with the final transaction result or instructions to follow, the display text "Remove Card" shall be displayed first.
- 2-4.8.1.16 B When performing
- a Capture or
 - a Supplementary Authorization or
 - a Reversal (Authorization)
 - A Cancellation
- no interaction between the cardholder and the terminal is requested, and only the Message Code '0E' ("Please Wait") shall be displayed on the Cardholder Display.
- NOTE:** The cardholder may need to sign a printed receipt before or during a Capture, but this is not interpreted as direct interaction.

- 2-4.8.1.17 A When the "CANCEL" (Slet Alt) key has been activated, message code 'E7' ("Purchase interrupted") shall be displayed on the Cardholder Display.
- 2-4.8.1.18 C When the receipt is being printed, message code 'E6' ("Printing receipt") shall be displayed on the Cardholder Display.

2-4.8.2 Audio Indicator

The audio indicator helps the cardholder know out whether a transaction was approved or rejected. The design requirements for the audio indicator can be found in section 2-6.2.6. The following requirements defines which events shall initiate an audio signal.

- 2-4.8.2.1 B An audio indicator shall emit a signal in order to indicate that the transaction is completed successfully.
- 2-4.8.2.2 B An audio indicator shall emit a signal in order to indicate that the transaction is failed/rejected.
- 2-4.8.2.3 B An audio indicator shall emit a signal in order to indicate that the card has not been removed while the display prompts the cardholder.
- NOTE:** The time-out before the signal is emitted may depend on the actual implementation and environment.
- 2-4.8.2.4 B If the volume of the audio indicator is adjustable, a separate volume control shall be implemented when indicating card not removed, see requirement 2-4.8.2.3.
- 2-4.8.2.5 C The audio indicator may also signal other events e.g. when activating numeric or function keys.

2-4.8.3 Cardholder Key Pad

The terminal contains a set of command keys in order to e.g. confirm the entry of a PIN. See section 2-6.2.9 for details. The command keys are not as such part of the PIN Pad.

2-4.8.4 Printer

Receipts

- 2-4.8.4.1 A The User Interface printer shall at least support printing of the receipts defined in section 1-12.
- 2-4.8.4.2 A Receipts shall be printed according to section 1-12 page 1-12-1.

2-4.9 Merchant Application Handler

2-4.9.1 Log

- 2-4.9.1.1 A The Log shall support all log activities.

- 2-4.9.1.2 A The MAD-Handler shall control all logging activities except the logging of the "Advice to Log".
- 2-4.9.1.3 A The MAD-Handler shall have access to a Log.
NOTE: The Log may be implemented as a "paper-journal" and/or electronically stored as a data file.
- 2-4.9.1.4 A If the log is stored on an electronic media, it shall be done in a 'non-cyclic' way, meaning that the log shall not overwrite previously written records.
- 2-4.9.1.5 A If the Log is not ready to store another entry, it shall not be possible to initiate a transaction.
- 2-4.9.1.6 A An entry in the Log shall as a minimum contain available transaction information, i.e. a copy of the transaction data printed on the corresponding receipt.
NOTE: Fixed data elements, e.g. ME_{NUMBER} and ID_{PSAM}, need not be repeated for each log entry unless the information is necessary to identify the specific terminal.
- 2-4.9.1.7 A Data logged shall conform to PCI ref. 37.
NOTE: See also section 1-7 page 1-7-1.
- 2-4.9.1.8 A In case of one log being shared by several terminals, it shall be unambiguously stated which terminal has generated which transaction log entry.
- 2-4.9.1.9 C If other relevant information is available it may be stored together with the associated transaction or with a reference to the transaction.
NOTE: Relevant information could be information about the goods and services paid for.
- 2-4.9.1.10 A If an error occurs during a transaction, the ASW1-ASW2 shall be printed/saved as part of the Log.

2-4.9.2 Serial Ports

This sub-handler need not be implemented to support the applications defined in this specification.

2-4.9.3 Merchant Display

- 2-4.9.3.1 A If Transaction State Information is requested by the terminal (indicated in "Info Level" in the *Exchange Debit/Credit Information* command), the terminal shall convey the information given by the PSAM to the attendant.
The following requirements, 2-4.9.3.2 and 2-4.9.3.3, are only relevant for an attended POS Terminal.
- 2-4.9.3.2 C In case of an unsuccessful transaction, the ASW1-ASW2 values may be displayed as four hexadecimal digits on the Merchant Display when available.
NOTE: The code may enhance the information seen from the merchant's perspective.

- 2-4.9.3.3 B Action Codes and error messages on the Merchant Display shall be displayed until the attendant actively deletes the message, e.g. by pressing a cancel key.

NOTE: The aim of this requirement is to make the Merchant aware of an error situation. If this is due to Merchant action, this requirement does not apply.

2-4.10 PSAM Handler

2-4.10.1 Interface to the PSAM

Introduction

Although the PSAM communicates with several other *logical* units, its only *physical* connection is to the PSAM Handler in the CAD.

- 2-4.10.1.1 A The PSAM interface must implement ref. 8: "ISO/IEC-7816-3" as detailed below.

NOTE: An interface fulfilling the requirements of ref. 20: "EMV ICC Specification" will not fulfil all requirements for the PSAM interface.

Power Supply

All PSAMs can operate in Class-A (5.0 V). Based on the hardware of the specific PSAM used, it may additionally operate in Class-B (3.0 V) and Class-C (1.8 V).

For example, PSAMs version 60 and 61 operate in Class-A and Class-B where PSAMs version 70 and 71 operate in Class-A, Class-B and Class-C.

According to ref. 8: "ISO/IEC 7816-3", the PSAM interface shall be able to deliver the following supply currents:

- Class-A: 60 mA
- Class-B: 50 mA
- Class-C: 30 mA.

- 2-4.10.1.2 A Class selection shall be performed as defined in ref. 8: "ISO/IEC 7816-3".

The current PSAM platforms consume up to approx. 20 mA when active (irrespective of the actual supply voltage). Whenever the PSAM is not processing a command, it will enter a sleep mode with a substantially lower power consumption. This sleep mode is controlled by the PSAM itself and requires no action from the PSAM interface.

Clock Frequency

- 2-4.10.1.3 A Unless another maximum clock frequency is specifically indicated in the ATR, the PSAM interface must provide a clock signal between 1 MHz and 5 MHz.

NOTE: The highest clock frequency possible should be used to obtain the fastest data transmission.

Transmission Protocol

- 2-4.10.1.4 A The PSAM interface shall implement the T=1 protocol (T=0 need not be supported).

Protocol and Parameter Selection (PPS)

- 2-4.10.1.5 B As the PSAM supports several sets of communication parameters (protocol type, F and D), the PSAM interface must use PPS as defined in ref. 8: "ISO/IEC 7816-3" to select which parameters to use (unless the default values of F = 372, D = 1 are used).
- 2-4.10.1.6 B The PSAM will indicate its maximum supported communication speed in TA1 of the ATR. The PSAM interface should select this communication parameter set if supported. Otherwise, it should successively try to select supported values with lower and lower communication speed until supported by the PSAM.

Supported Transmission Speeds

The current PSAMs all support the following communication parameters (all T=1):

- F = 372, D = 1
- F = 372, D = 2
- F = 372, D = 4
- F = 372, D = 12

Future PSAMs may additionally support more combinations, such as:

- F = 372, D = 20
- F = 372, D = 32

Information Field Size for the Interface Device (IFSD)

The information field size for the interface device (IFSD) is the maximum length of the information field of blocks that can be received by the PSAM interface.

- 2-4.10.1.7 B The information field size for the interface device shall be 254 bytes in order to speed-up the transaction, and this size shall be used until the PSAM is powered off.
- 2-4.10.1.8 B Consequently, the first block sent by the terminal following the PPS (if performed) shall be an S(IFS request) with IFSD = 254. Otherwise, a default size of 32 will be used by the PSAM.

NOTE: The information field size for the PSAM (IFSC) is given in the ATR and must be respected.

Waiting Time Extension (WTX)

- 2-4.10.1.9 A Although not used in present PSAM versions, Wait time Extension shall be supported.

Empty I-Blocks

- 2-4.10.1.10 A The PSAM interface shall support I-blocks with a length of 0 bytes. This requirement complies with ref. 8: "ISO/IEC 7816-3" but is not required in ref. 20: "EMV ICC Specification".

2-4.10.2 Commands between the CAD and the PSAM

Commands and responses are exchanged between the terminal and the PSAM. The terminal sends commands to the PSAM which replies with the corresponding responses. However, the PSAM may, in order to fulfil its tasks, respond with one or more commands to other handlers before responding to the original command. Each of the commands from the PSAM are embedded in special responses in order to comply with the transmission protocol. Likewise, responses from other handlers to the PSAM are embedded in special commands.

- 2-4.10.2.1 A The CAD shall in addition to the TAPA defined commands, support the commands defined in table 2-14.1 page 2-14-1 as necessary for the applications supported (debit/credit).

2-4.11 Data Store Handler

2-4.11.1 Data Store

The PSAM stores transaction information in the Data Store. When EMV cards are used for debit/credit transactions, a Financial Advice is stored, whereas for MSC debit/credit transactions, a Financial Advice is stored in the case of an offline transaction only.

- 2-4.11.1.1 A The Data Store Handler shall comply with ref. 27: "TAPA, Application Architecture Specification".
- 2-4.11.1.2 B When writing to the Data Store, the Data Store Handler shall ensure that the data *written* actually are stored in the Data Store before responding successfully.
- 2-4.11.1.3 B The Data Store Handler shall contain an error detection feature in order to discover unintended alteration in data during storage. If alteration has occurred, an Advice Transfer shall be initiated according to the requirements given in section 2-5.15.3 page 2-5-104.
- 2-4.11.1.4 C The Data Store Handler may contain an error correction feature in order to recover unintended alteration in data during storage.

2-4.12 Communication Handler

2-4.12.1 General Requirements

- 2-4.12.1.1 A The Communication Handler shall comply with ref. 27: "TAPA, Application Architecture Specification".

- 2-4.12.1.2 A Any time-out defined between the terminal and cash register for a business call shall take into regard the worst case scenario with regards to no online response.

2-4.13 Event Handler

2-4.13.1 General Requirements

- 2-4.13.1.1 A The Event Handler shall comply with ref. 27: "TAPA, Application Architecture Specification".

2-4.14 New PIN Synchronization

2-4.14.1 General Requirements

This section describes a new way of handling PIN encryption keys synchronization. This is an extension to the requirements found in ref. 27: "TAPA, Application Architecture Specification".

- 2-4.14.1.1 A A terminal without a PED (PIN pad) shall use the synchronization flow as specified in in ref. 27: "TAPA, Application Architecture Specification".
- 2-4.14.1.2 A A terminal with a PED and the new PIN key scheme shall in the *Set Debit/Credit Properties* command, with an identifier of scheme '80 01', set bit b7 in Terminal settings to indicate that it supports the new PIN Synchronization scheme.

A new PSAM will recognize the new bit in the Terminal Settings and respond positively with a soft ASW = '10AB' (PTS Activated). An old PSAM will ignore the new bit in the Terminal Settings and respond positively with ASW='0000'.

In this way, the terminal can determine whether the PSAM supports the new synchronization method. The terminal may decide not to proceed if it detects a mismatch in PIN synchronization capabilities between the PED and PSAM. The PSAM will, if the synchronization is not successful, not proceed with the installation and generate an ASW = '1001'.

2-4.14.2 Key Generation Requirements

- 2-4.14.2.1 A The terminal supplier shall, when requesting initial keys for the PED at least supply the following information;
- ID_{PPCREATOR} (supplier identifier)
 - ID_{PP} (device serial number)
- The latter may be provided as a range of numbers.

2-4.14.3 Key derivation

The following operators are used in this section:

- $||$ = The concatenation operator,
- $!$ = the 1's complement (or bitwise NOT) operator.

- 2-4.14.3.1 A A PED shall, when it receives Key Encryption Key, KEK, derivation data, derive the KEK from the Master Key, MK_{PED} in the following way:
- $KEK_{PED} = [Deriv. data]_{MK,PED}$ where;
- $Deriv. data = VK_{PED,KEK} || TS_{PED,KEK} || !VK_{PED,KEK} || !TS_{PED,KEK}$
- $VK_{PED,KEK}$ = PED KEK version number, 4 bytes
- $TS_{PED,KEK}$ = PED KEK Date (Time stamp), 4 bytes
- 2-4.14.3.2 A A PED shall, when it receives an encrypted BDK decrypt it using the KEK_{PED} .
- 2-4.14.3.3 A A PED shall derive the Basic Session Key, BSK_{PED} from the System Derivation Key in the following way:
- $BSK_{PED} = [RND_{SESS} || NT_{PIN} || !RND_{SESS} || !NT_{PIN}]_{SDK}$
- where;
- RND_{SESS} = Random number, 4 bytes
- NT_{PIN} = PIN Transaction counter, 4 bytes
- 2-4.14.3.4 A The PED shall diversify the Basic Session Key in the following way;
- The Session Key for PIN encryption, PSK, shall be computed by logically bit-wise XOR'ing the BSK with Mask1.
 - The Session Key for data encryption, DSK, shall be computed by logically bit-wise XOR'ing the BSK with Mask2.
 - The Session Key for MAC computation, MSK, shall be computed by logically bit-wise XOR'ing the BSK with Mask3.
- Where;
- Mask 1 = '00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 FF'
- Mask 2 = '00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 FF 00'
- Mask 3 = '00 00 00 00 00 00 FF 00 00 00 00 00 00 00 FF 00 00'
- 2-4.14.3.5 A The PED shall, if a PIN related CDP key is used, derive the CDP key in the following way;
- $CDP_{PED} =$
 $['FF FF FF FF 00 00 00 00 FF FF FF FF 00 00 00 00 ']_{SDK}$
- No further diversification shall be performed. This corresponds to a BSK with a transaction counter of '00 00 00 00' and a Random Number of 'FF FF FF FF'. This key will be unique as the transaction counter never will be zero.
- 2-4.14.3.6 A A PED shall, to avoid replays attacks, perform the following validations;
- Validate that the Key version, $VK_{PED,KEK}$ is the same or larger than the current value stored in the PED
 - Decrypt the BDK and calculate the KCV_{BDK} .
 - Only store the KEK derivation data, the KEK_{PED} and the SDK if the KCV_{BDK} has been verified to be equal to the value received in the command from the PSAM.

2-4.15 Card Data Protection

2-4.15.1 Introduction

Card Data Protection (CDP) is mandatory to implement in order to establish a secure zone between the Card Reader and PSAM.

Further information can be found in ref. 40: "Nets Design Report: Card Data Protection".

- 2-4.15.1.1 A Card Data Protection shall be implemented.

2-4.15.2 CDP Implementation

CDP can be implemented in three ways:

- Based on the TAPA PIN scheme, using a PKI and deriving KEY_{CDP} from $KSESS_{INIT}$ in the Secure Device (SD),
- Based on the new PIN scheme in section , deriving the KEY_{CDP} from the SDK,
- Using a KEY_{CDP} previously loaded into a secure Card Reader.

If the PKI method is used, it requires that the terminal has a SD and also that the Card Reader is a part of the SD. The same key hierarchy used to establish the secure zone between the PSAM and PIN Pad is used to derive the KEY_{CDP} .

If the terminal uses the new PIN scheme is used, then the key derivation shall be performed as specified in section 2-4.14.

If the keys can be exchanged from PSAM in a secure way then one of these methods is recommended.

The other method where a KEY_{CDP} is loaded into a secure Card Reader requires additional CDP key management taken care of by the terminal vendor.

- 2-4.15.2.1 A One of the methods described above shall be implemented.

2-4.15.3 Key Management - KEY_{CDP} from a secure Card Reader

If a KEY_{CDP} from a secure Card Reader is used, this KEY_{CDP} has to be loaded into the PSAM. This has to be done in a secure way using a KEK_{CDP} .

This requires that the secure Card Reader has been personalized with a $[KEK_{CDP}]KEK_{CDP,ini}$ where the KEK_{ini} is a top level key provided by Nets as split keys.

When a secure Card Reader has been personalized it will contain: $[KEK_{CDP}]KEK_{CDP,ini}$, $[KEY_{CDP}]KEK_{CDP}$, KEY_{CDP} .

The KEY_{CDP} has to be loaded into the PSAM to establish the secure zone. This is done by first sending the $[KEY_{CDP}]KEK_{CDP}$ to the PSAM. If it is first time the PSAM "connects" to this Card Reader the PSAM will reject the load command because the KEK_{CDP} is unknown to the PSAM. In this case the $[KEK_{CDP}]KEK_{CDP,ini}$ shall be sent to the PSAM and after this $[KEY_{CDP}]KEK_{CDP}$.

After each Startup of the PSAM the $[KEY_{CDP}]KEK_{CDP}$ shall be sent to the PSAM to ensure that both Card Reader and PSAM agrees on which KEY_{CDP} to use.

2-4.15.4 Enabling CDP mode in the PSAM

Enabling the CDP mode in the PSAM is done issuing a *Set D/C Properties* command with Id = '8001' (Terminal Settings).

The bits b3 and b2 in Terminals Settings are used to enable the CDP mode. The bits b3 and b2 also defines if CDP is enabled both ways or only from Card Reader to PSAM.

If CDP is enabled from PSAM towards the Card Reader the PSAM will only encipher commands (TAPA commands where MT = '48') if they contain sensitive data (E.g. PAN, Track2 etc.).

Terminal Settings also defines if new TAPA PIN Block format shall be used and if response to TAPA commands where MT = '48'/'47' shall be in plaintext (even in CDP mode). CDP mode can only be disabled during an installation of the PSAM.

2-4.15.5 Generating of CDP Session Key ($KSES_{CDP}$)

The key used for enciphering of the messages is a session key derived from the KEY_{CDP} . TAPA defines how the $KSES_{CDP}$ is derived from the KEY_{CDP} .

2-4.15.6 Using the $KSES_{CDP}$

$KSES_{CDP}$ is used for enciphering of all responses from the ICC (EMV transactions) and for enciphering the Track2 Data and Key Entered Data when initiating a MSC or Key Entered transaction.

$KSES_{CDP}$ is also used for enciphering of the Track input to *Get D/C Properties* command with Id = '0012'.

NOTE: The response to the *Select* command will not be enciphered. See section 2-4.15.8 below for further exceptions.

2-4.15.7 Private Label MSC recognition in CDP mode

As the terminal may not know the MSC tracks in plaintext and MSC tracks should not be exposed on an unprotected PSAM interface, it is not possible to use *Get D/C Properties* command with Id = '0002' to have the PSAM to check if a MSC is recognized as a Private Label Card.

Instead a *Get D/C Properties* command with Id = '0012' shall be used which takes enciphered tracks as input. If Track2 is recognized as Private Label Card or validated to be "non ISO" coded the Tracks input will be returned in plaintext.

2-4.15.8 Get Last ICC Response handling in CDP mode

In the case where the PSAM ask for the FCI issuing a *Get Last ICC Response* command, the FCI was originally sent in clear text (response to Select command).

In this case the PSAM will send the "Get Last ICC Response" addressing the '0202' handler to get the response also in clear text.

2-4.15.9 Verify Offline PIN handling in CDP mode

The Verify Offline PIN command is sent in either a TAPA MT = '46' or TAPA MT = '47' command depending on if old or new format of the PIN block has been implemented.

The TAPA commands with MT = '46' or TAPA MT = '47' contents are routed via the SD to the Card handler. The enciphered response from the Card handler will return to the SD to be MAC'ed.

In CDP mode the input to the MAC calculation is: Seed □ Enciphered data from ICC □ MAC from command.

2-4.15.10 Check Stop List handling in CDP mode

The purpose of the Check Stop List command (issued by the PSAM) is that the terminal can check the full PAN in a Stop List and indicate in the response whether the card was black-listed or not.

However, in CDP mode the PAN has been truncated so only 6 + 4 digits are visible. In this case the only purpose of the Check Stop List command is to return an Authorization Code to the PSAM.

2-4.16 Terminal Initialization

This section describes the initialization process common to all applications.

2-4.16.1 Reset of the CAD

- | | | |
|------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-4.16.1.1 | A | Initialization of the CAD shall be done automatically after power-on. |
| 2-4.16.1.2 | A | It shall be possible to provoke a reset of the CAD by use of a service function. This service function may be initiated from the Merchant Application. |

2-4.17 Fallback from ICC to Magnetic Stripe

2-4.17.1 Introduction

This section defines the requirements for handling the fallback from ICC to magnetic stripe.

The requirements defined by the card schemes define that the ICC has first priority and should be attempted read three times when handling cards equipped with both an ICC and a magnetic stripe.

- 2-4.17.1.1 A As defined by the Card Schemes, using the ICC shall have first priority. The ICC shall be attempted read three times before the terminal may fall back to magstripe when handling cards equipped with both ICC and magstripe.

Also, the requirements defined by the card schemes define that fallback transactions shall be online processed, and that fallback transactions may not be accepted in all environments.

2-4.17.2 General Requirements

The reading of card data, and the application selection are performed by the terminal (MAD-Handler) which shall comply with the requirements below for handling fallback from ICC to magnetic stripe.

- 2-4.17.2.1 A The terminal shall always attempt to perform the transaction with the ICC first.

- 2-4.17.2.2 A If the response to *Initiate MSC Payment* command tells that the Service Code is either '2xx' or '6xx', the terminal shall instruct the merchant and the cardholder to use ICC reader.

NOTE: The response to *Initiate MSC Payment* command will tell if the Service Code on the magnetic stripe shows that an ICC is present on the card by.

- 2-4.17.2.3 A The terminal shall attempt to retry reading the ICC 3 times prior to initialize a fallback transaction, e.g. by requiring the cardholder to insert/reinsert the chip card 3 times.

NOTE: Terminals with motorized readers should attempt to restage the card in the ICC reader or retract and re-land the ICC contacts.

- 2-4.17.2.4 A If all the mutually supported Debit/Credit applications are blocked, then fallback to magnetic stripe shall not be initiated.

- 2-4.17.2.5 A If the transaction is cancelled before completion, either by the merchant or the cardholder, the ICC shall still be the priority and the counter of ICC attempts shall be reset, i.e. fallback to magnetic stripe shall not be initiated.

- 2-4.17.2.6 A Fallback in attended environments shall require the merchant to initiate this transaction type actively, e.g. by pressing a specific button.

- 2-4.17.2.7 A If the card is removed during ATR or Application Selection, the terminal shall return to state idle and the counter of ICC attempts shall be reset.
- 2-4.17.2.8 A The terminal shall prevent the possibility of provoking a fallback transaction deliberately by prematurely removing the card three consecutive times.
- 2-4.17.2.9 A The terminal shall set the value for POS Entry Mode, position 3 to '7' for a fallback transaction.

Fallback - separate card readers

- 2-4.17.2.10 A Terminals with separate readers shall be able to guide the merchant and/or the cardholder to use either of the readers in case of fallback situations.

In figure 2-4.2 page 2-4-28, a flag called 'ICC Reader Tried' has been introduced. This flag shall control the situations when an ICC card has been swiped/inserted in a separate magnetic stripe reader without previous attempt to use the ICC reader.

Since the PSAM is validating the Service Code from the magnetic stripe, the terminal shall first try to initiate a normal magnetic stripe transaction before performing a fallback transaction. The response from PSAM will indicate if an ICC is present and is first priority.

- 2-4.17.2.11 A When separate readers are utilized, the merchant shall confirm (physically) that the card was inserted correctly and that initiation of fallback is accepted.

NOTE: An example of the message displayed at the Merchant Display could be: "Card inserted correctly?".

- 2-4.17.2.12 C The functional requirements may be implemented as shown in the figures 2-4.1 page 2-4-27 to 2-4.5 page 2-4-32.

Figures 2-4.1 page 2-4-27 to 2-4.5 page 2-4-32 show the procedures for handling fallback from ICC technology to magnetic stripe technology for separate readers.

If the cardholder follows the guidelines given by the display, the "ICC Reader Attempt Counter" will be incremented and fallback will be offered after three attempts, only.

Fallback - combined card readers

- 2-4.17.2.13 A When a combined reader is utilized in an attended environment, the merchant shall confirm (physically) that fallback may be initiated.

NOTE: An example of the message displayed at the Merchant Display could be: "Continue using mag-stripe?".

- 2-4.17.2.14 C The functional requirements may be implemented as shown in in the figures 2-4.1 page 2-4-27 to 2-4.7 page 2-4-33.

NOTE: When PSE is supported, additional handling may be necessary (command etc.), e.g. to check whether blocked applications exist in the card or not.

The figures 2-4.5 page 2-4-31 and 2-4.6 page 2-4-32 shows the procedures for handling fallback when the magnetic stripe is read before reading the ICC.

Figures 2-4.6 page 2-4-32 and 2-4.7 page 2-4-33 shows the procedures for handling fallback when the ICC is read before the magnetic stripe.

2-4.17.3 Final Decision

The PSAM will - possibly based on the response from the authorization system - decide whether or not a fallback transaction can be initiated.

- 2-4.17.3.1 A The terminal shall use the ASW1-ASW2 codes given in the responses from the PSAM to verify that fallback is allowed.
- 2-4.17.3.2 B Only if reading of the ICC has been attempted three times, the terminal may initiate a fallback transaction when the ASW1-ASW2 = '1222' (Service Code: ICC to be used) in the response to the *Initiate MSC Payment* command.
- 2-4.17.3.3 B The terminal may initiate a fallback transaction if the ASW1-ASW2 has one of the values '10FB' or '10FD' in response to the *Complete Payment* command.
- 2-4.17.3.4 B The terminal may initiate a fallback to a contact transaction if the ASW1-ASW2 has the value of '10FC' in response to the *Complete Contactless Payment* command.

NOTE: The requirements in section 2-4.17.2 shall be observed before acting on these ASWs.

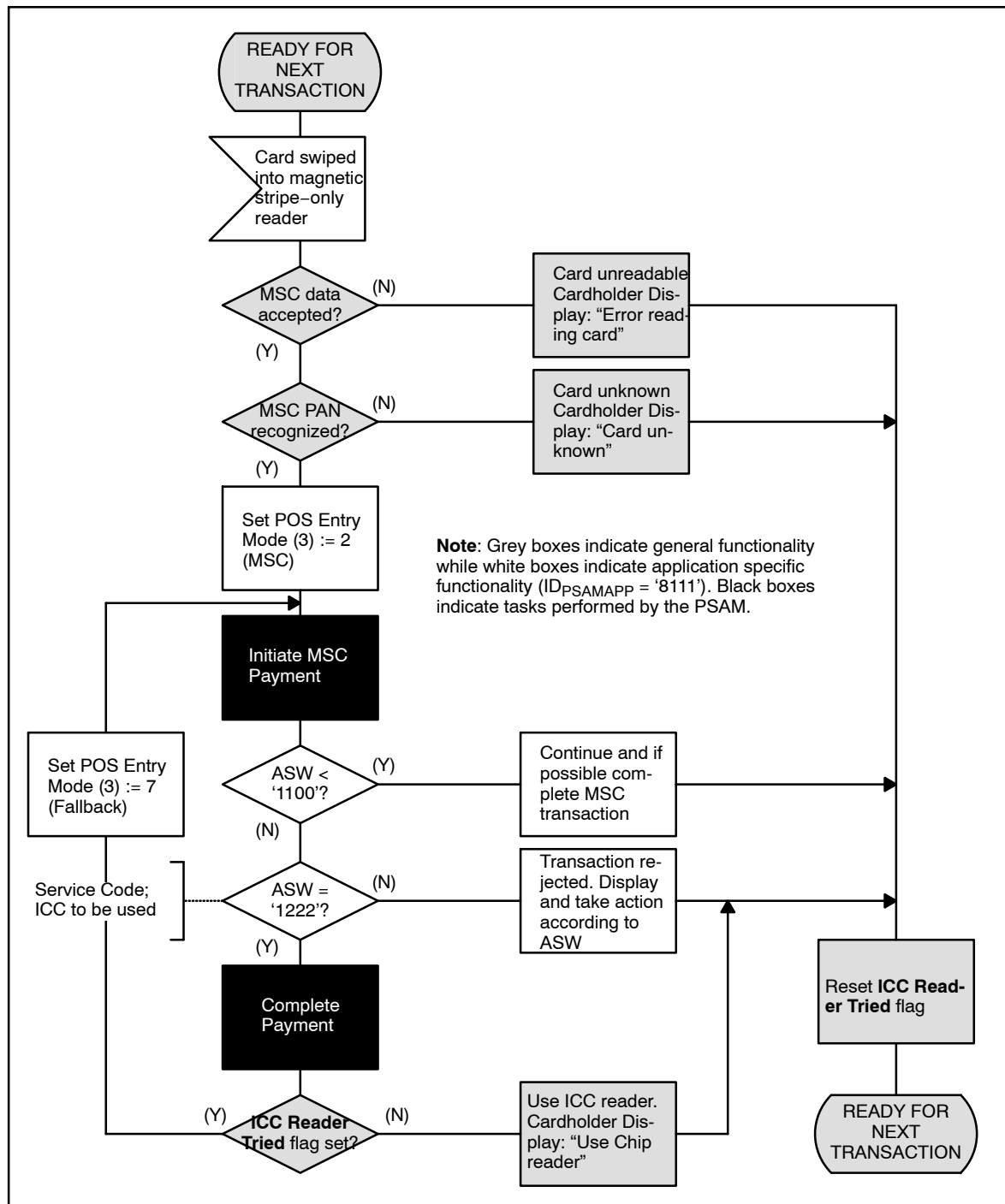


Figure 2-4.1 - Fallback Handling - Magstripe (Separate Readers)

- 2-4.17.3.5 C It is recommended that the time-out value shown in figure 2-4.2 page 2-4-28 is configurable. Initial value to be selected may be 15 sec.

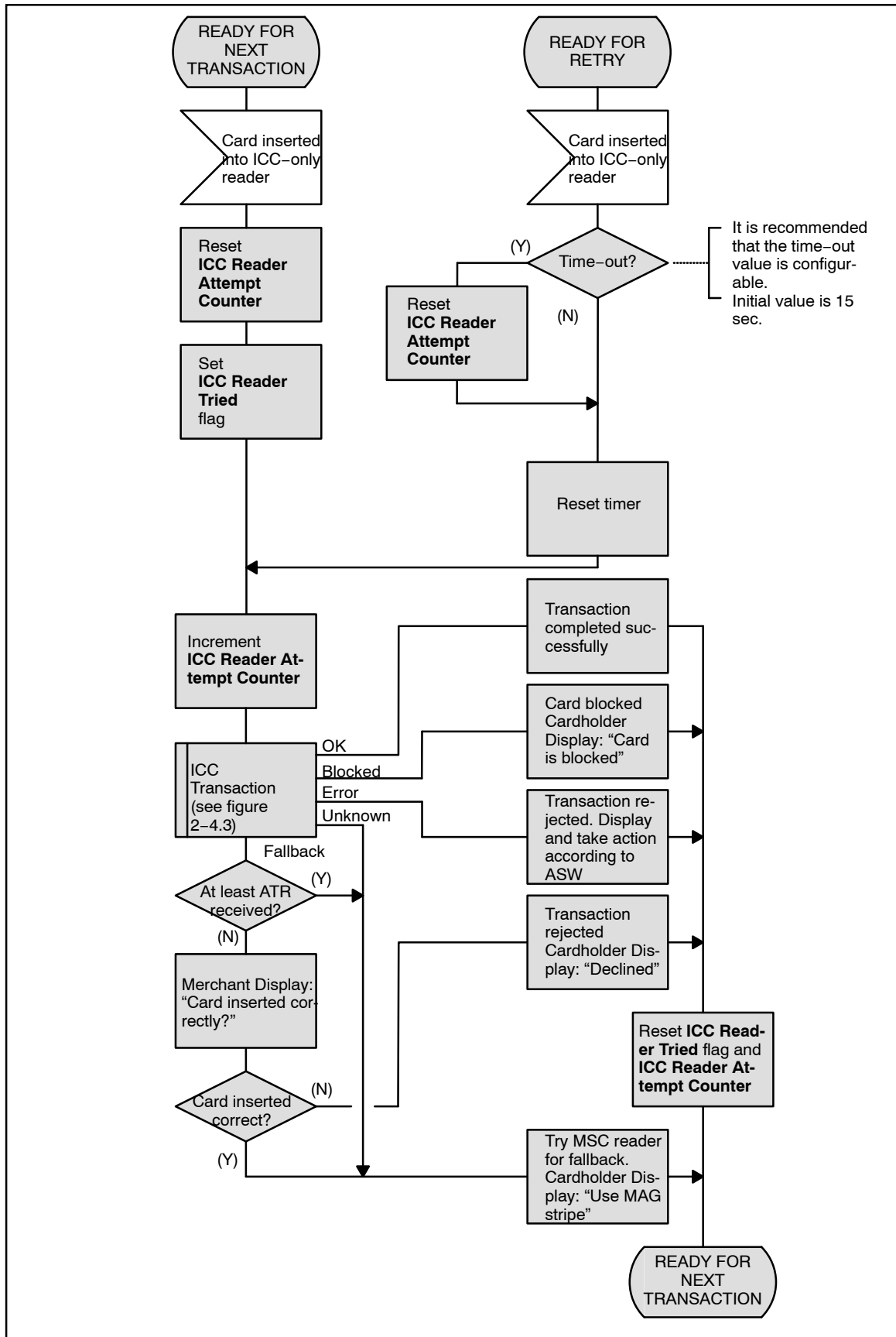


Figure 2-4.2 - Fallback Handling - ICCR (Separate Readers)

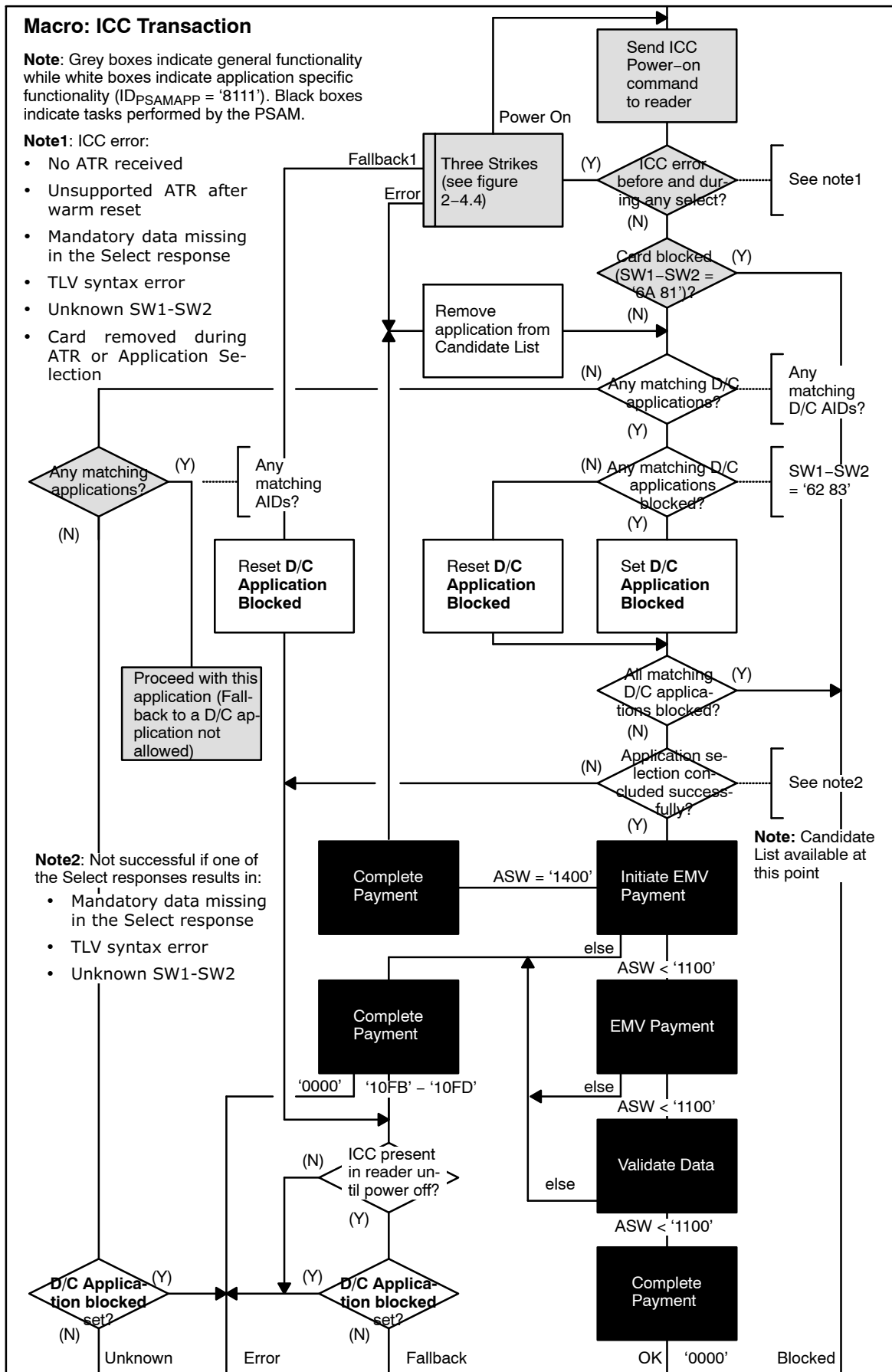


Figure 2-4.3 - Fallback Handling - ICC Transaction

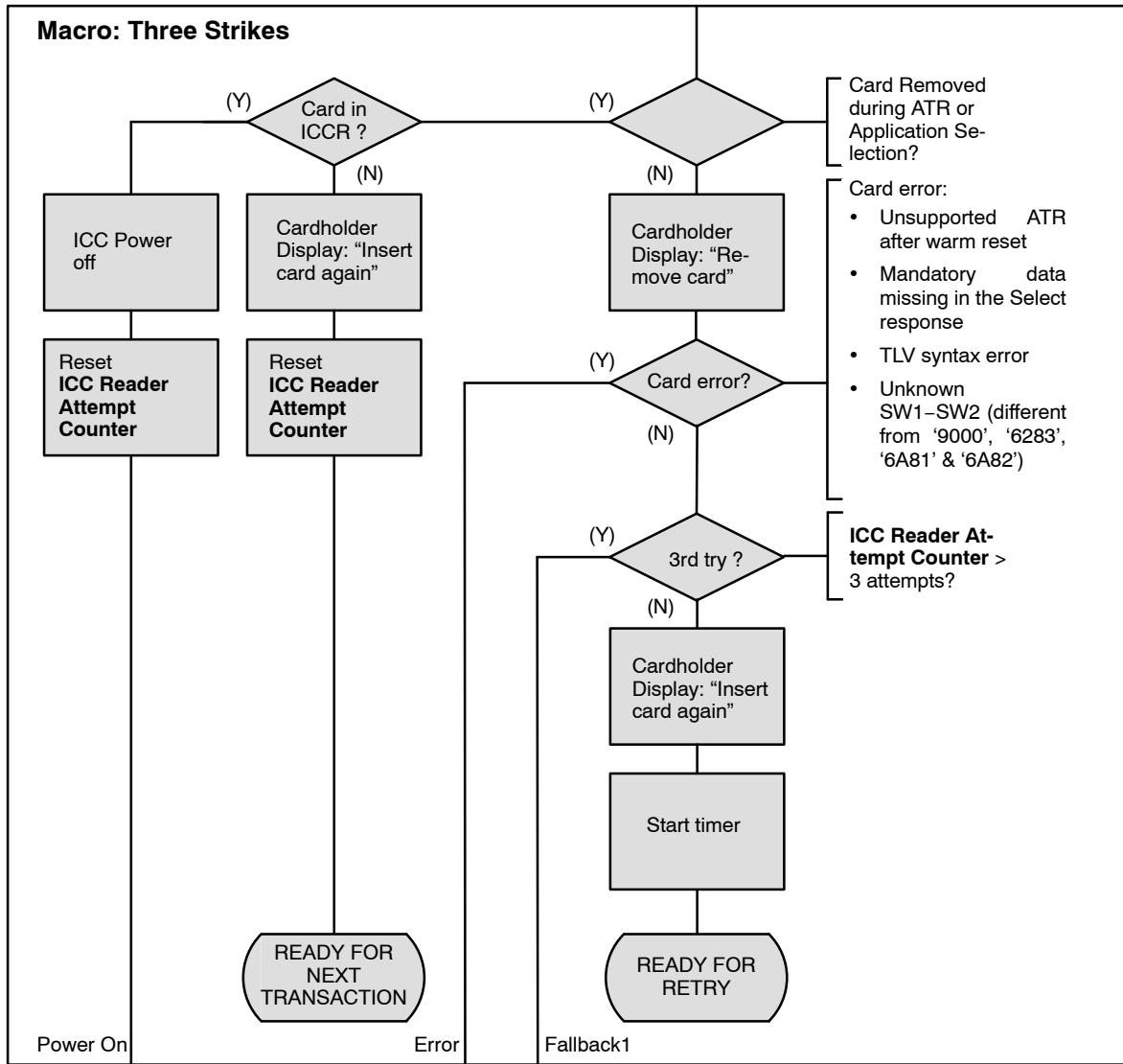


Figure 2-4.4 - Fallback Handling - Three Strikes

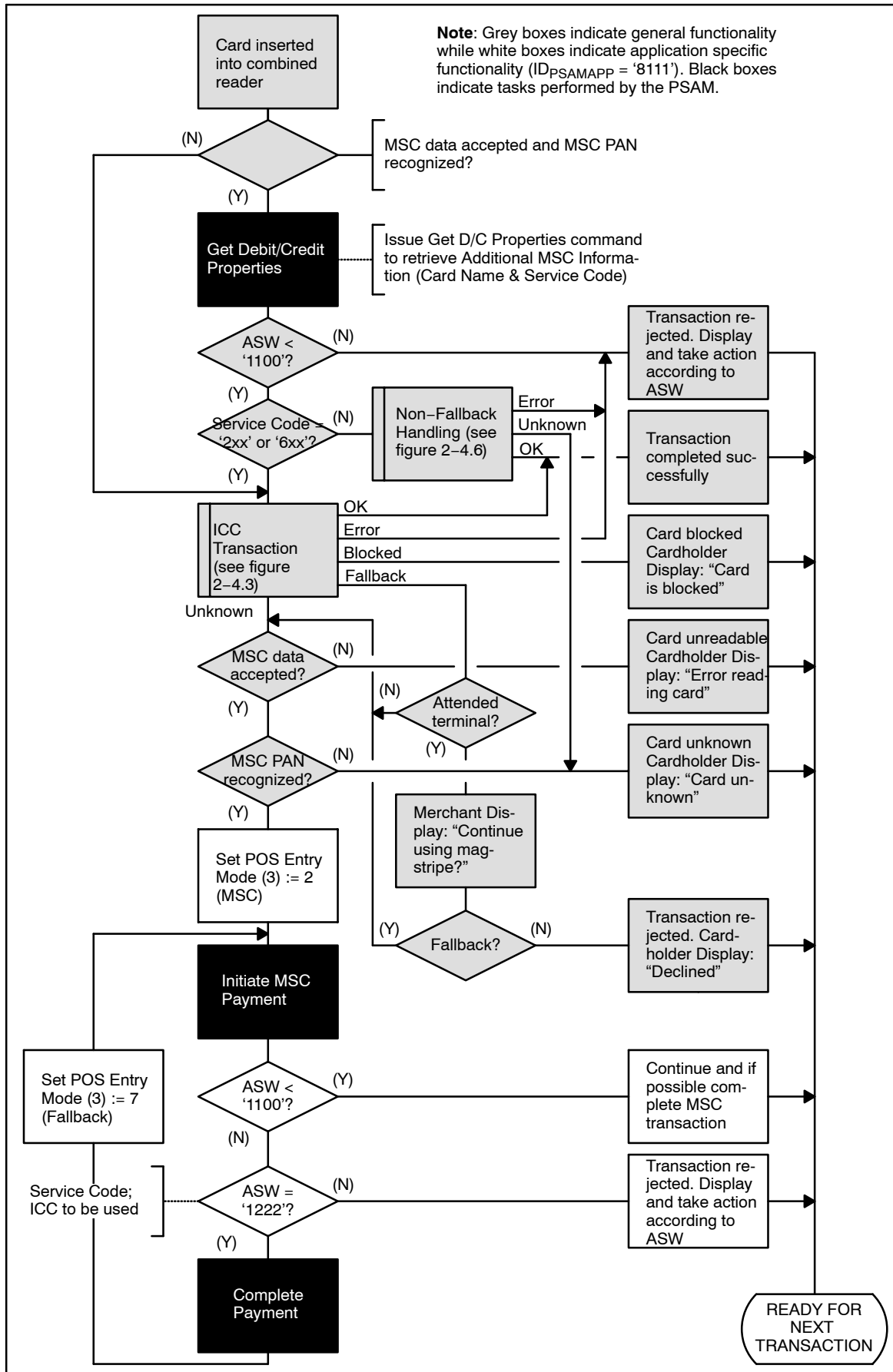


Figure 2-4.5 - Fallback Handling (Combined Readers) - MSC read before ICC

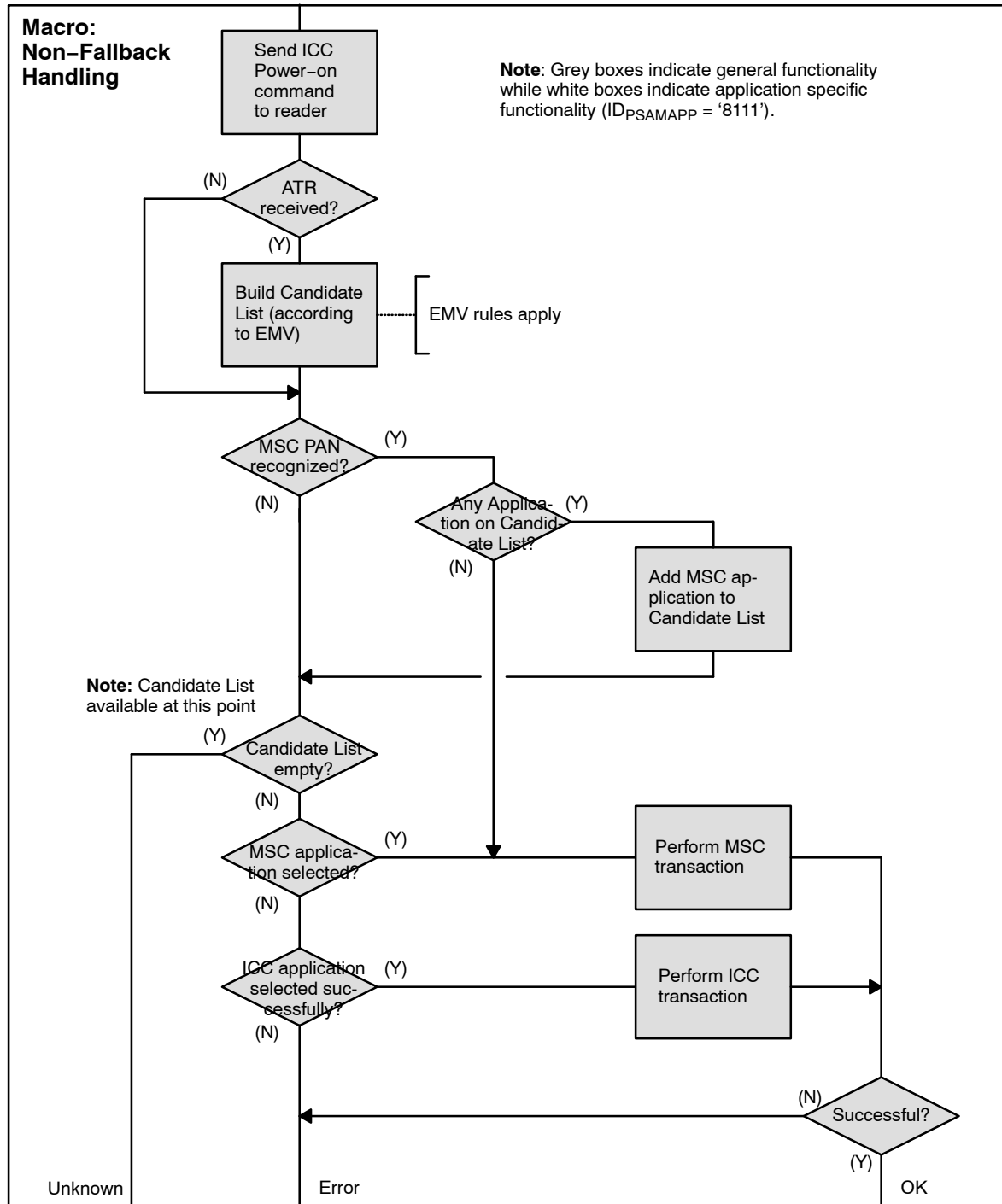


Figure 2-4.6 - Non-Fallback Handling (Combined Readers)

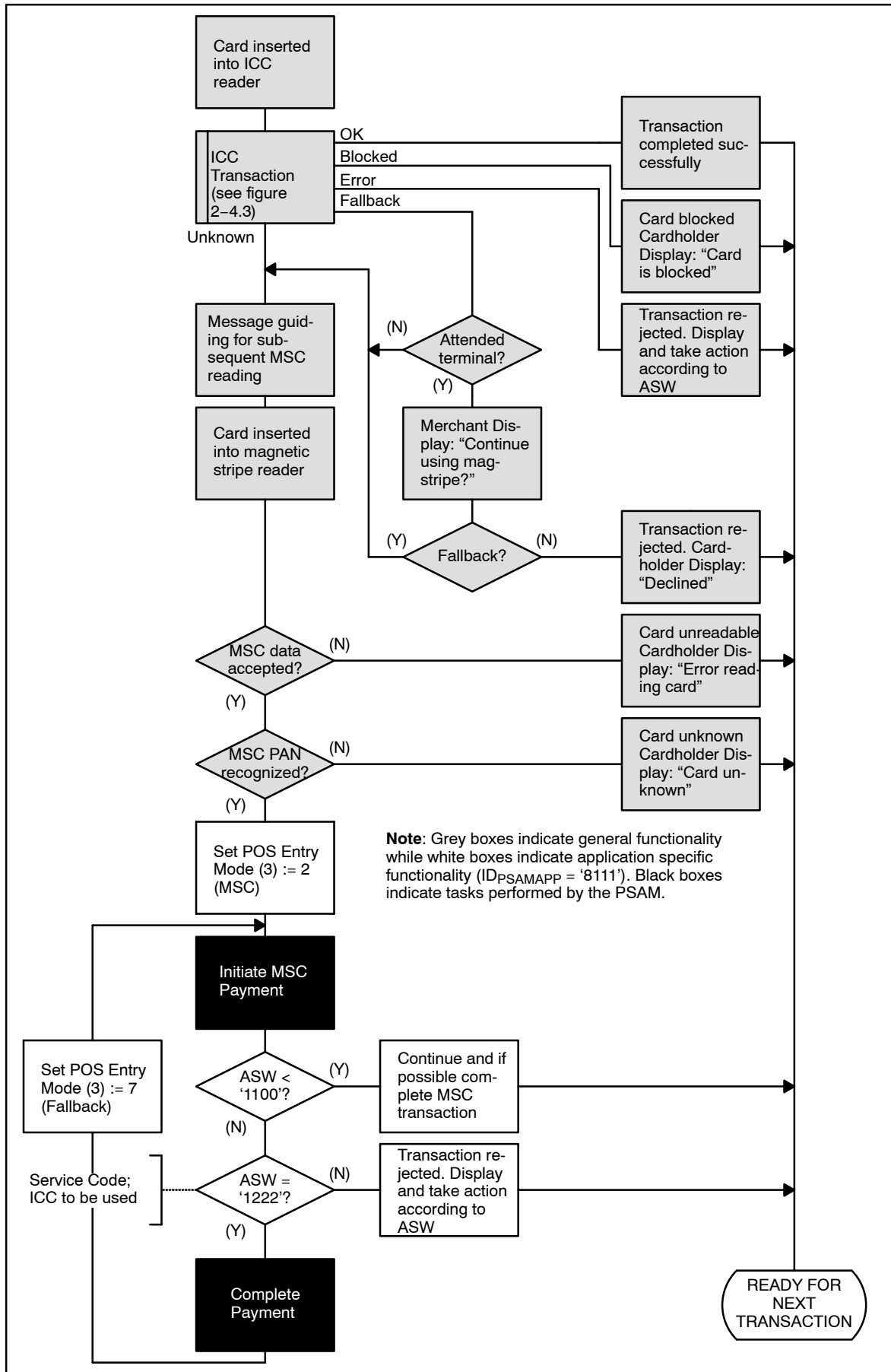


Figure 2-4.7 - Fallback Handling (Combined Readers) - ICC read before MSC

2-4.18 Counters and Batch Numbers

2-4.18.1 Introduction

The following counter related data elements are available in Financial Responses (Financial Request Response or Financial Advice Response) and Reversal Advice Responses:

- **Reconciliation counter id** (field 44). Indicates a numeric link to the relevant counter for the card sent in the request/advice.
- **Reconciliation counter name** (field 44). Indicates an alphanumeric link to the relevant counter for the card sent in the request/advice.
- **Reconciliation date** (field 28).
- **Reconciliation indicator** (field 29). Subdivision of field 28.

The data related to the counters are listed in table 2-4.5. Examples of values for Reconciliation counter id and Reconciliation counter name can be found in section 2-13.9.10.

2-4.18.2 Batch Number

The Batch Number (Retrieval Reference Number, field 37) is maintained by the merchant.

See also section 1-9.25, Guidelines for Constructing Total Reports.

NOTE: The Batch Number may be indicated at the statement of account. However, some acquirers may rewrite the value, e.g. truncate the number of characters printed. Please refer to processing rules defined by the acquirer.

- 2-4.18.2.1 A A given Batch Number shall only contain transactions made in a single currency.

NOTE: When a Batch Number shall be selected or an algorithm for issuing Batch Numbers shall be defined, the following issues should be taken into considerations:

- The Batch Number should be unique over a period of time (e.g. 12 months).
- The Batch Numbers should be unique for each terminal within a shop (i.e. under the same Merchant Number).
- Based on the Batch Number, the actual currency should be identifiable.

Table 2-4.5 - Data Available for Counter Purposes (Example)

Data delivered by:					
Terminal		Acquirer			
Batch Number (37)	Transaction Currency (49)	Reconciliation counter id (44)	Reconciliation counter name (44)	Reconciliation date (28)	Reconciliation indicator (29)
" 208960"	208 (DKK)	003	UDL.EC/MC/VI/JCB	000312	001
" 208960"	208 (DKK)	005	DINERS	000312	002
" 752961"	752 (SEK)	003	UDL.EC/MC/VI/JCB	000313	001

The principles used in this example is based on the following assumptions:

- The Batch Number consists of 6 digits only,
- The 3 most significant digits define the currency,
- The 3 least significant digits constitute an index.

Other principles may be more convenient like e.g.:

- The Batch Number consists of 6 digits only,
- 2 digits identify the terminal within the shop,
- 1 digit identifies the currency,
- 3 digits constitute an index.

This page is intentionally left blank

2-5 Debit/Credit Functionality

2-5.1 Application Initialization

2-5.1.1 Introduction

- 2-5.1.1.1 A After the CAD is powered on, communication between the CAD and the PSAM shall be established according to the description in ref. 27: "TAPA, Application Architecture Specification".
- 2-5.1.1.2 A Initialization of the debit/credit application shall be established as defined in figure 2-5.1 page 2-5-3 and described in the following requirements.

There are five different initialization steps:

- **Restart:** first step after the PSAM has been powered on
- **Installation:** used when the PSAM is not already installed properly
- **New Application Data:** used when new data has been sent to the PSAM, such as new AIDs or PAN ranges
- **Configuration:** used when configuration is requested by the PSAM
- **PSAM/PIN Pad Synchronization:** to establish a synchronization between the PSAM and PIN Pad

Start-up with a New PSAM

The first time a PSAM is inserted in a terminal, the following sequence will be requested:

- **Restart**
- **Installation**
- **New application data**
- **Configuration**
- **PSAM/PIN Pad synchronization**

Start-up (Normal Procedure)

A typical restart sequence of the PSAM requires only the following mandatory sequence:

- **Restart**
- **PSAM/PIN Pad synchronization**

The number of initialization steps depends on the ASW1-ASW2 received from the PSAM. Therefore, additional steps may be requested.

- 2-5.1.1.3 A If more PSAMs are present for handling debit/credit transactions, initialization shall be performed for each of these PSAMs.
- 2-5.1.1.4 A The ID_{PSAMAPP} for the debit/credit application (indicated in P1, P2 of the commands) shall be '8111'.

NOTE: The following requirements only concern initialization of a single PSAM.

2-5.1.2 Power On

- 2-5.1.2.1 A If needed, the MAD-Handler shall apply power to and reset the PSAM by sending the *ICC Power-On* command to the relevant PSAM Handler.

NOTE: This step shall not be performed if the PSAM has already been powered on to initialize another application.

- 2-5.1.2.2 A If no PSAM was present during power-on, the PSAM Handler shall perform an *ICC Power-On* command when the PSAM is inserted and post this event (Chip Card Inserted, location '00pp') to the Event Handler.

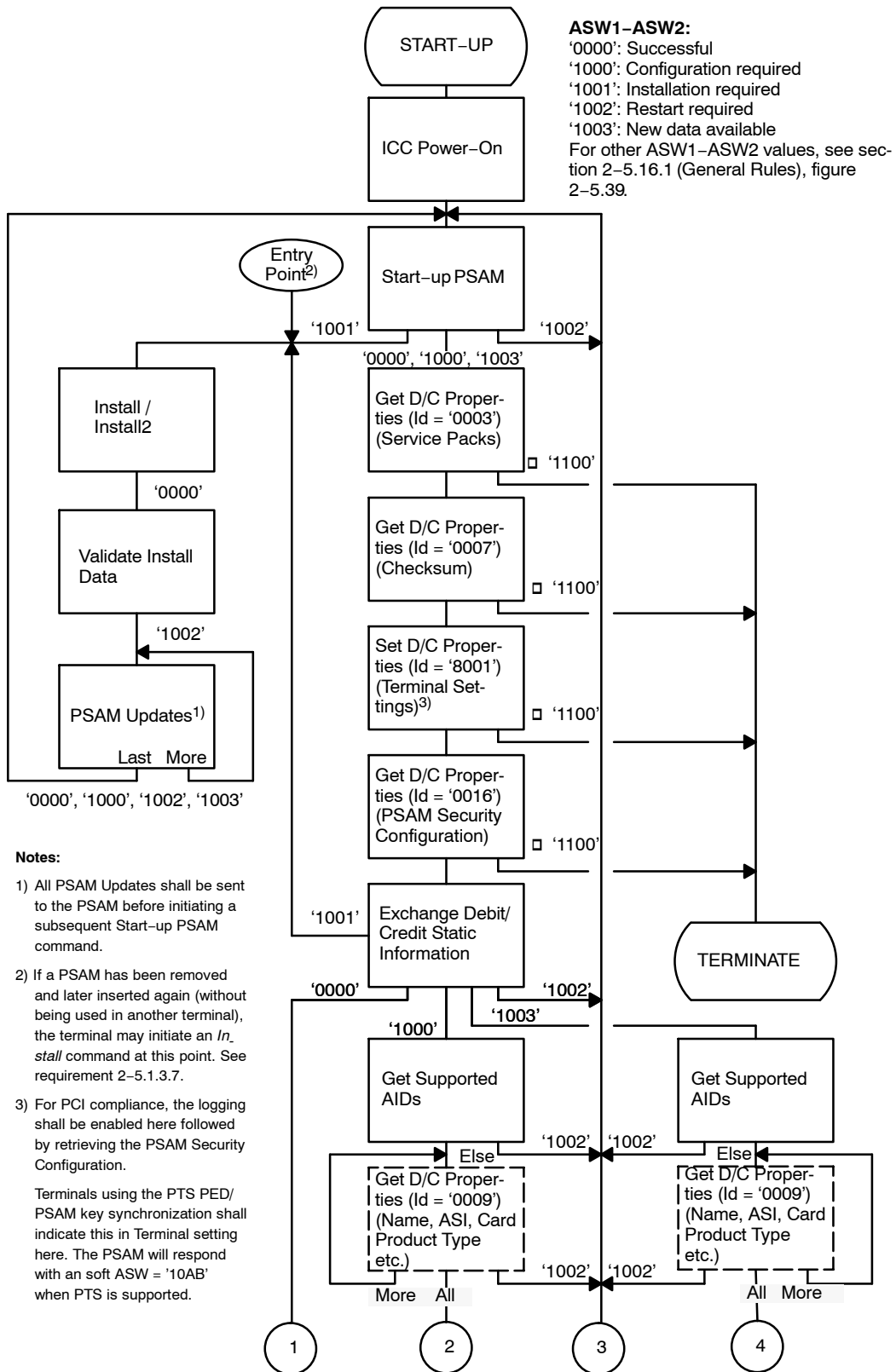
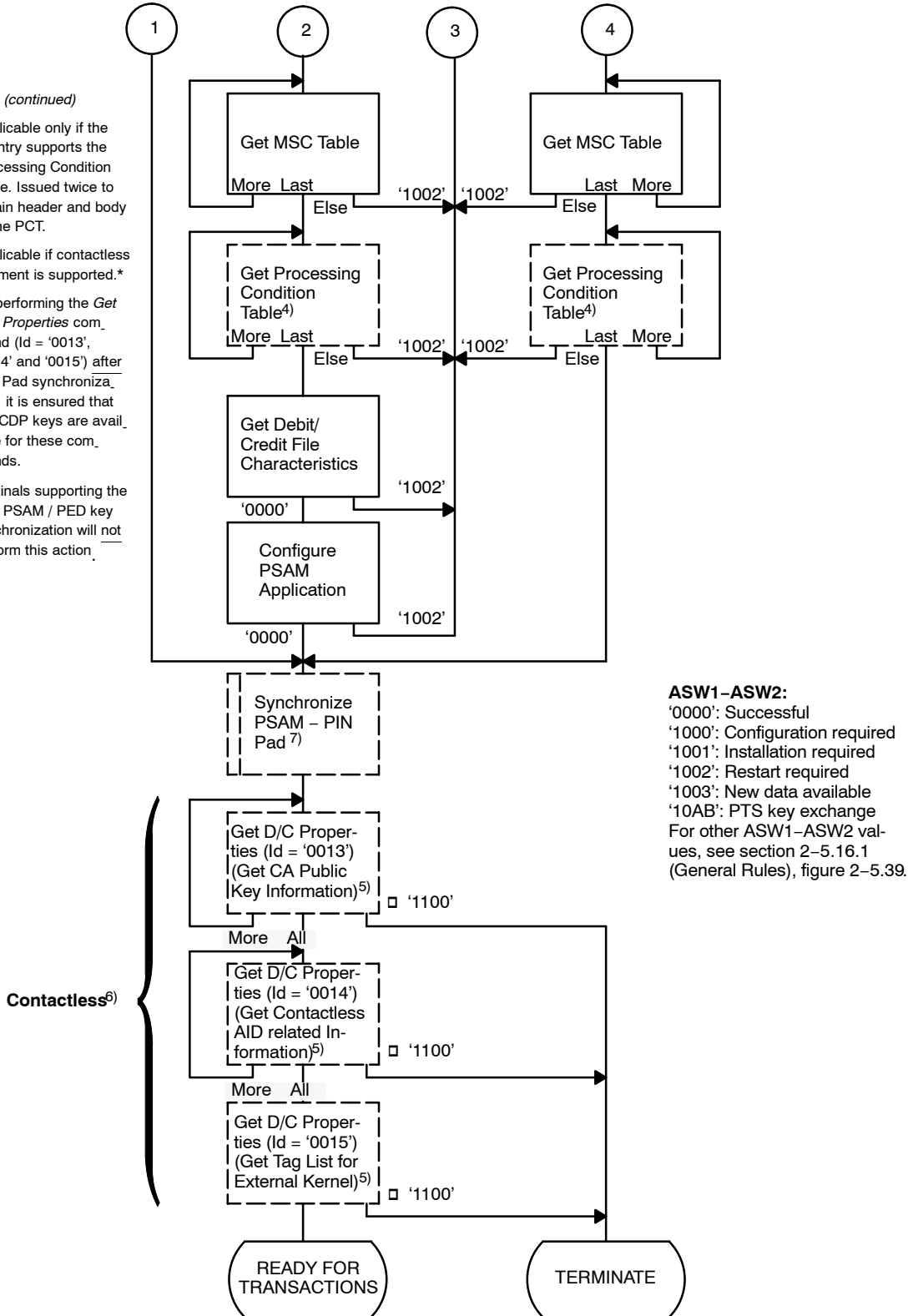


Figure 2-5.1 - Initialization Sequence - Normal Flow

Notes: (continued)

- 4) Applicable only if the country supports the Processing Condition Table. Issued twice to obtain header and body of the PCT.
- 5) Applicable if contactless payment is supported.*
- 6) By performing the *Get D/C Properties* command (Id = '0013', '0014' and '0015') after PIN Pad synchronization, it is ensured that the CDP keys are available for these commands.
- 7) Terminals supporting the PTS PSAM / PED key synchronization will not perform this action.



ASW1-ASW2:
 '0000': Successful
 '1000': Configuration required
 '1001': Installation required
 '1002': Restart required
 '1003': New data available
 '10AB': PTS key exchange
 For other ASW1-ASW2 values, see section 2-5.16.1 (General Rules), figure 2-5.39.

Figure 2-5.1 - Initialization Sequence - Normal Flow (concluded)

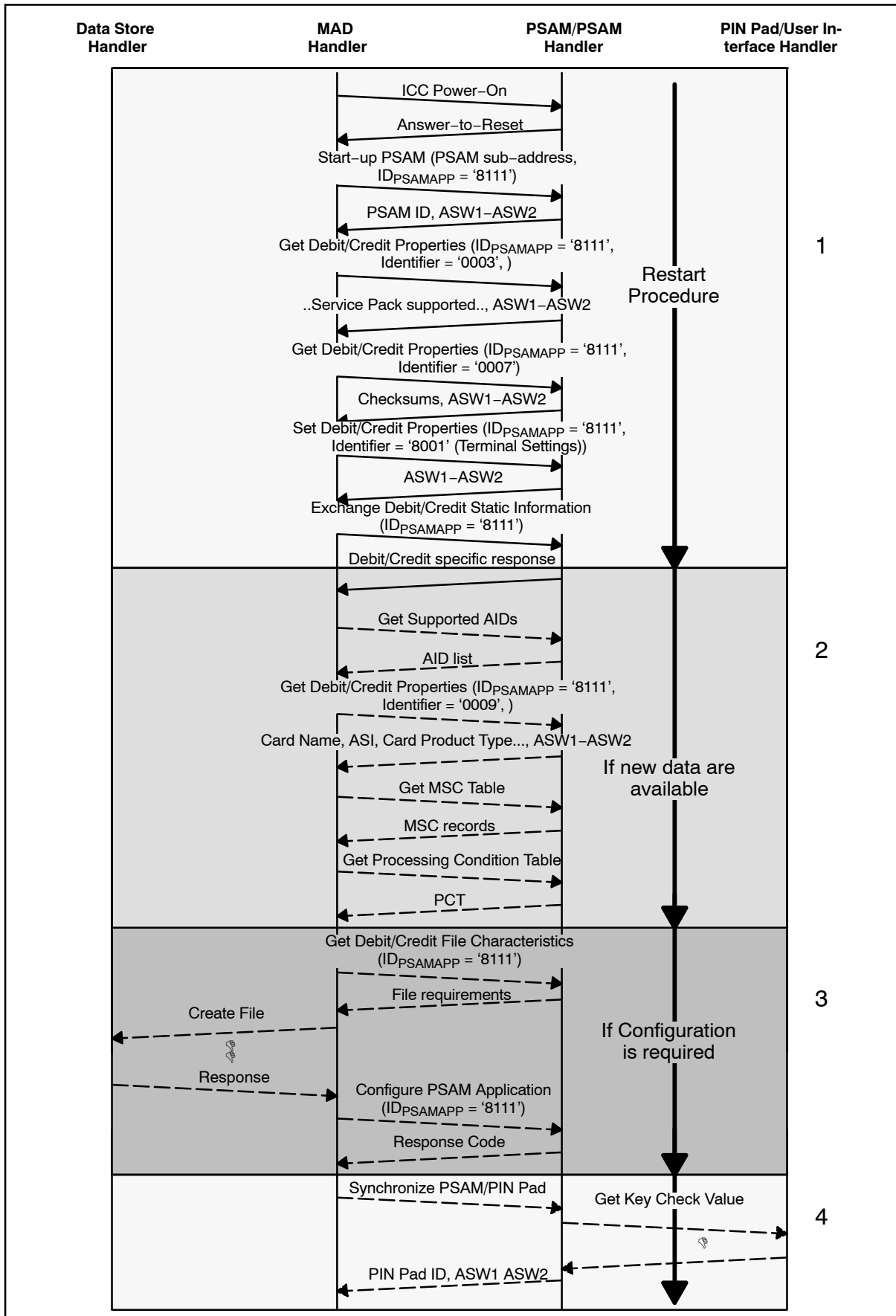


Figure 2-5.2 - PSAM Debit/Credit Application Initialization Sequence (without Installation)

2-5.1.3 Restart

A typical Restart sequence of the PSAM Debit/Credit application requires these commands in the listed order :

- *Start-up PSAM* (PSAM Identification)
- *Get Debit/Credit Properties* (Service Packs)
- *Get Debit/Credit Properties* (Checksums)
- *Set Debit/Credit Properties* (Terminal Settings)
- *Exchange Debit/Credit Static Information*

Start-up PSAM

- 2-5.1.3.1 A The MAD-Handler shall send the *Start-up PSAM* command to the PSAM after receiving the ATR and PPS. The command shall contain the sub-address assigned to the reader in which the PSAM is inserted.
- 2-5.1.3.2 A The MAD-Handler shall retain the PSAM Identification returned by the PSAM along with the assigned sub-address.
- 2-5.1.3.3 A Based on the ASW1-ASW2 received in the *Start-up PSAM* response, the MAD-Handler shall determine whether:
- The Restart sequence shall be re-initiated (ASW1-ASW2 = '1002')
 - The Installation sequence shall be initiated (ASW1-ASW2 = '1001')
 - The Restart sequence shall continue (ASW1-ASW2 = '0000', '1000' or '1003')
- 2-5.1.3.4 A If ASW1-ASW2 has the value '0000' (Successful), reading of PSAM data is optional and file configuration shall *not* be performed.
- 2-5.1.3.5 A The *Exchange Debit/Credit Static Information* and *Synchronize PSAM/PIN Pad* command shall be issued before the terminal is ready to perform debit/credit transactions.
- NOTE:** By reading the PSAM data even when the ASW1-ASW2 has the value '0000', the terminal is guaranteed to operate with the most up to date data.
- 2-5.1.3.6 A If ASW1-ASW2 has the value '1000' (Configuration required), reading PSAM data *and* performing file configuration shall be performed.
- NOTE:** If the PSAM indicates that configuration is required for the PSAM debit/credit application, then no transactions will be accepted until the configuration process is complete.
- 2-5.1.3.7 A If ASW1-ASW2 has the value '1001' (Install transaction required), an installation transaction shall be performed before further initialization can be performed.
- NOTE:** If a PSAM has been removed from a terminal and later on inserted again (without being used in another terminal), the PSAM does not require an Installation transaction. Even though the PSAM does not require an Installation transaction, the terminal may initiate the *Install* command. If the terminal detects that the PSAM has been substi-

tuted, an Installation transaction may be relevant or desirable.

- 2-5.1.3.8 A If ASW1-ASW2 has the value '1002' (Restart required), the *Start-up PSAM* command shall be resent.
- 2-5.1.3.9 A If ASW1-ASW2 has the value '1003' (New data available), reading PSAM data is mandatory and performing file configuration shall not be performed.

Service Packs

Before any transaction can be performed, the terminal and the PSAM must agree upon the level of Service Pack to be used. Additional information can be found in section 2-8 (Service Packs)

- 2-5.1.3.10 A Immediately after the response to the *Start-up PSAM* command, the MAD-Handler shall send a *Get Debit Credit Properties* command with Identifier = '0003'. The response will indicate which Service Packs the PSAM supports.
- 2-5.1.3.11 A The terminal shall support at least Service Pack 2.
- 2-5.1.3.12 A The MAD-Handler shall choose the highest mutual supported Service Pack No. This number shall be indicated in Terminal Approval Number sent in the succeeding *Exchange Debit/Credit Static Information* command.

NOTE: How to select the highest mutually supported Service Pack No. is explained in figure 2-5.3 page 2-5-8.

- 2-5.1.3.13 A If the response to the *Get Debit/Credit Properties* command indicates either:
- unknown command (ASW1-ASW2 = '1122', INS not supported) or
 - unknown value of Identifier (ASW1-ASW2 = '10ED', Identifier not supported)
- the terminal shall interpret these responses as “no Service Packs supported”.

NOTE: If the terminal has been approved to support multiple Service Packs, the terminal may request any of the mutually supported Service Packs.

- 2-5.1.3.14 A If the Service Pack No. requested by the terminal, does not match the Service Packs supported by the PSAM, the terminal shall interrupt the start-up procedure.

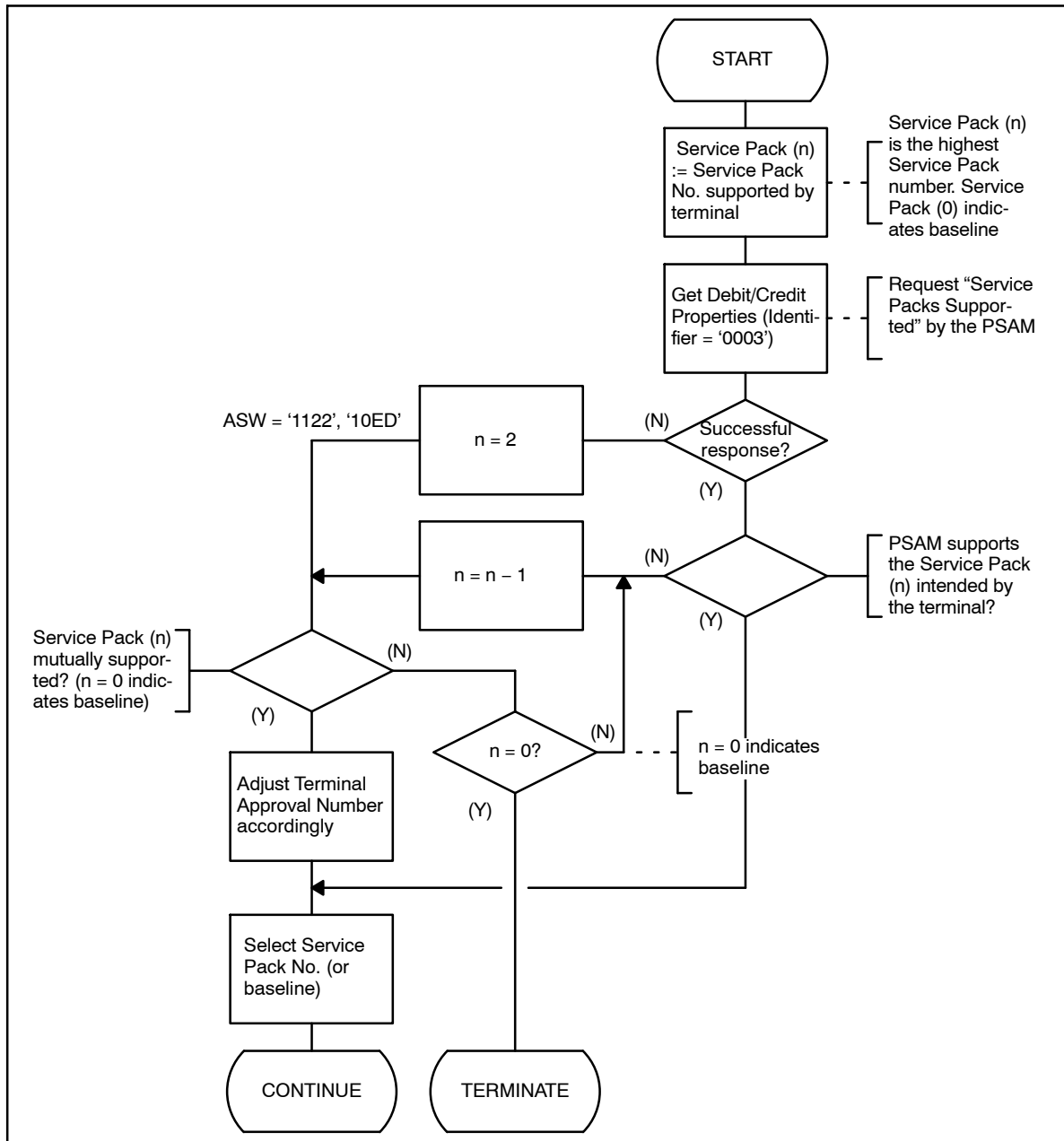


Figure 2-5.3 - Service Pack Check

2-5.1.3.15 A The Terminal Approval No. (3 MSB) shall be adjusted according to the Service Pack selected.

Set Debit/Credit Properties

2-5.1.3.16 A The MAD-handler shall issue a *Set Debit/Credit Properties* (ID = '8001') command to the PSAM to retrieve the PSAM Security configuration.

2-5.1.3.17 A The MAD-handler shall send the terminals configuration in the Terminal Settings.
The PSAM will return a ASW of '10AB' if it supports PTS.

Exchange Debit/Credit Static Information

2-5.1.3.18 A The MAD-Handler shall send the *Exchange Debit/Credit Static Information* command to the PSAM.

- 2-5.1.3.19 A Based on the ASW1-ASW2 received in the *Exchange Debit/Credit Static Information* response, the MAD-Handler shall determine whether:
- The Restart sequence is completed (ASW1-ASW2 = '0000')
 - The New Application Data and Configuration sequence shall succeed (ASW1-ASW2 = '1000')
 - The Installation sequence shall be initiated (ASW1-ASW2 = '1001')
 - The Restart sequence shall be re-initiated (ASW1-ASW2 = '1002')
 - The New Application Data sequence shall succeed (ASW1-ASW2 = '1003')
- In the response to the *Exchange Debit/Credit Static Information* command, the PSAM will furthermore provide merchant relevant data.
- 2-5.1.3.20 A The terminal shall contain one merchant table with the contents given in table 2-5.1. The merchant table is used when printing.

Table 2-5.1 - Terminal Merchant Table

Data element	Value	Length
ME No.	Merchant number	5
ME _{NAME}	Merchant name	18
ME _{CITY}	Merchant city	16
ME _{ADDRESS}	Merchant address	24
ME _{ZIP}	Merchant zip code	8
ME _{PHONE}	Merchant Phone No.	24
ME _{BRN}	Merchant Business Registration Number	12

Merchant Application Log

If the Merchant Application supports logging functions, the MAD-Handler may request the PSAM to deliver the logging information. The following logging information will be available (if requested):

- A copy of Financial Advices stored in Data Store, except for the Message Reason Code (field 25) which indicates "Backup message".
- A copy of Reversal Advices stored in Data Store, except for the Message Reason Code (field 25) which indicates "Backup message".

- 2-5.1.3.21 A The MAD-Handler shall indicate whether logging information delivered by the PSAM is requested or not. This is indicated in "Info Level" in the *Exchange Debit/Credit Static Information* command.

NOTE: The way the MAD-Handler is informed of the backup logging capabilities is outside the scope of this specification.

PSAM State Information

In order to keep the merchant informed of the tasks performed by the PSAM, the MAD-Handler may request PSAM State In-

formation. This information makes it possible for the merchant to monitor if e.g. the PSAM waits for the cardholder to key in the PIN. The information will be conveyed in the *Transaction State Information* command.

NOTE: An unsuccessful response to the *Transaction State Information* command will be ignored by the PSAM.

- 2-5.1.3.22 A The MAD-Handler shall indicate whether PSAM State Information shall be sent to the Merchant Application or not. This is indicated in "Info Level" in the *Exchange Debit/Credit Static Information* command.

Confirm Amount

- 2-5.1.3.23 A The MAD-Handler shall indicate whether the *Confirm Amount* command is requested for Original/Extended Authorizations or not. This is indicated in "Info Level" in the *Exchange Debit/Credit Static Information* command.

2-5.1.4 Installation

An Installation sequence requires these steps in the listed order:

- *Install* or *Install2*
- Installation Request (host message)
- *Validate Install Data*
- PSAM Update sequence (host messages)
- *PSAM Update*

The requirements concerning the Installation Transaction is listed in section 2-5.13.2 page 2-5-91, Installation Transaction.

- 2-5.1.4.1 A The *Install2* command shall be used if the terminal as well as the PSAM supports PTS.

The requirements concerning the PSAM Updates is listed in section 2-5.13.3 page 2-5-93 PSAM Update Transaction.

- 2-5.1.4.2 A If the response to *Validate Install Data* command is not successful, the installation procedure shall be interrupted, i.e. the PSAM Update sequence shall not be executed.

2-5.1.5 New Application Data

- 2-5.1.5.1 A If the PSAM has been updated with application data since last initialization (indicated by the ASW1-ASW2), the following commands shall be performed after the *Exchange Debit/Credit Static Information* commands:

- *Get Supported AIDs*
- *Get Debit/Credit Properties* (Identifier = '0009')
- *Get MSC Table*
- *Get Processing Condition Table*

The *Get Supported AIDs* command is used to update the list of supported AIDs in the terminal.

The *Get Debit/Credit Properties* command is used to retrieve a number of specific data elements per AID. The response

message is TLV-coded and the response will at least include the following mandatory data elements:

- DF70 - Card Name
- DF71 - ASI
- DF72 - Card Product Type

Additional data elements may be included:

- DF73 - Card Product Functions
- DF74 - Card Product Flow
- DF75 - Entry Point Parameters

NOTE: The tags 'DF73' to 'DF75' are mandatory for contactless (qVSDC) applications.

- 2-5.1.5.2 A The *Get Debit/Credit Properties* (Identifier = '0009') command shall be issued for all AIDs supported by the PSAM.

The *Get MSC Table* command is used to update the list of supported PAN ranges in the terminal.

The *Get Processing Condition Table* command is only applicable for countries supporting Processing Condition Table.

- 2-5.1.5.3 A The terminal shall issue the *Get Processing Condition Table* command twice in order to obtain the header and the body (containing the conditions).

- 2-5.1.5.4 A The terminal shall be able to handle TLV format.

NOTE: Terminals are already obliged to handle TLV format in the response to the *Select* command.

- 2-5.1.5.5 A If the "Continuation Indicator" in the response to the *Get MSC Table* command indicates that more MSC Table entries are available, the MAD-Handler shall re-issue the *Get MSC Table* command until every MSC Table entries has been retrieved.

NOTE: The PSAM may contain so much data that a *Get Next* command shall be submitted according to ref. 27: "TAPA, Application Architecture Specification".

2-5.1.6 Configuration

- 2-5.1.6.1 A When ASW1-ASW2 = '1000' (Configuration required) is returned in the response to either the *Start-up PSAM* or *Exchange Debit/Credit Static Information* command, the terminal shall issue the following commands:

- *Get Supported AIDs*
- *Get Debit/Credit Properties* (Identifier = '0009')
- *Get MSC Table*
- *Get Processing Condition Table*
- *Get Debit/Credit File Characteristics*
- *Configure PSAM Application*

See figure 2-5.1 page 2-5-3 for further details.

The *Get Debit/Credit File Characteristics* command is used by the terminal to retrieve the file usage information from the PSAM application, such that the MAD-Handler can allocate the amount of terminal data store space needed for this PSAM application.

The *Create File* command may be used by the MAD-Handler to create the number of files according to the requirements indic-

ated in the response to *Get Debit/Credit File Characteristics* command.

The *Configure PSAM Application* command is used by the MAD-Handler to inform the PSAM application of the actual file IDs reserved for the requested files.

2-5.1.7 PSAM/PIN Pad Synchronization

As the last step in the initialization sequence, the synchronization between the PSAM and PIN Pad(s) is performed. This is however only applicable if the Terminal and PSAM does not use the new PTS synchronization scheme, using the *Install 2* command.

- 2-5.1.7.1 A The following command shall, if synchronization has not been previously achieved during an *Install 2* command, be performed as the last command in the initialization sequence:
- *Synchronize PSAM/PIN Pad*
- 2-5.1.7.2 A The secure zone between the Nets PSAM and the PIN Pad shall be established according to ref. 27: "TAPA, Application Architecture Specification". For further details, see figure 2-5.4 page 2-5-13.
- 2-5.1.7.3 A The terminal shall perform a synchronization for each PIN Pad attached.
- 2-5.1.7.4 A The synchronization sequence shall be initiated by the terminal even though the terminal does not have a PIN Pad.
- 2-5.1.7.5 A If no PIN Pad is present, the Response Code shall be 'FFFB' (Unsupported operation) in the response to *Get Key Check Value* command.
- 2-5.1.7.6 A If the secure zone cannot be established, the terminal will only be able to perform Signature and No CVM based transactions.
- The synchronization sequence depicted in figure 2-5.4 page 2-5-13 will also be initiated by the PSAM each time an *Initialize Payment* command (requiring PIN) is issued as well.
- 2-5.1.7.7 A The PED shall, if the PSAM and the terminal has performed an *Install 2* command protect against a replay attack by validating the key validation data for the PED KEK. It shall validate that:
- The key version received is the same or one higher, than the value currently stored in the PED.
 - The time stamp received is the same, or higher, than the value currently stored in the PED.
 - The validation shall be performed before the PED starts to decrypt the SDK.
 - The PED shall only store the KEK Derivation Data, the KEK and the SDK if the KCV_{SDK} has been validated to be correct.
- Consequently, the initial key derivation data must be initialized to binary zeroes so the first real set of derivation data from the Host will be accepted.
- 2-5.1.7.8 A The PED shall not derive a PED KEK if the derivation data is zero. This will only be the situation until the first successful Installation transaction has been performed with a PSAM.

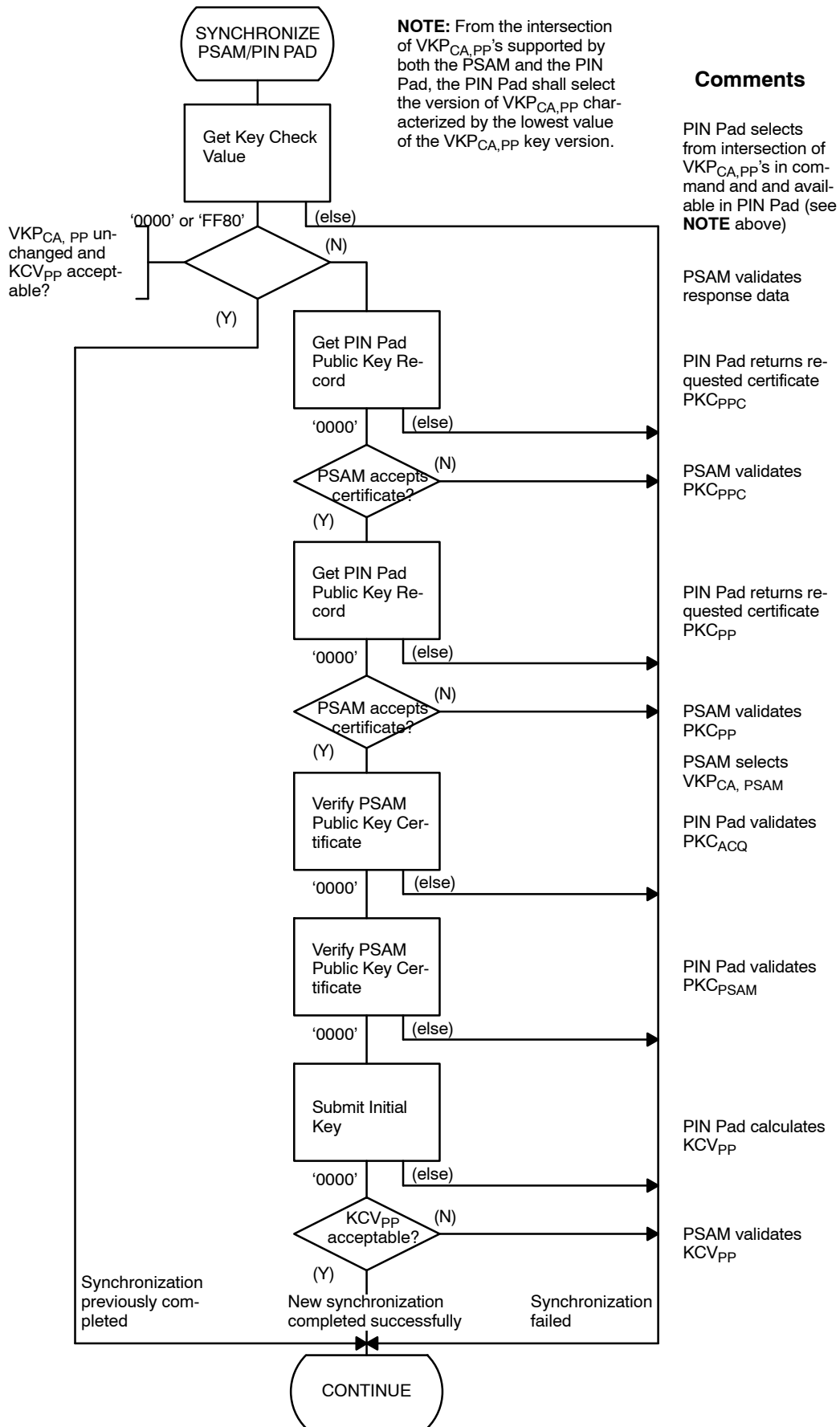


Figure 2-5.4 - Non-PTS PSAM/PIN Pad Synchronization Sequence

2-5.1.8 PSAM Shutdown

In order to speed-up the restart procedure, the *PSAM Shutdown* command may be used. This command allows the PSAM application to save all the outstanding data, prior to withdrawing power from the PSAM.

NOTE: Each PSAM application requires an individual *PSAM Shutdown* command.

- 2-5.1.8.1 A The *PSAM Shutdown* command shall conform to the format defined in ref. 27: "TAPA, Application Architecture Specification".

2-5.2 Stop List

2-5.2.1 Data Values used for Stop List Status

The Stop List Status command is used for two purposes;

- Check id a card is on a stop list,
- Entry of information from voice authorization.

Figure 2-5.5 page 2-5-15 shows the data values to use in the different situations.

The use of stop list check is not possible anymore, due to the PCI requirements of protection of cardholder information.

- 2-5.2.1.1 A Stop List Status shall be set according to figure 2-5.5 page.

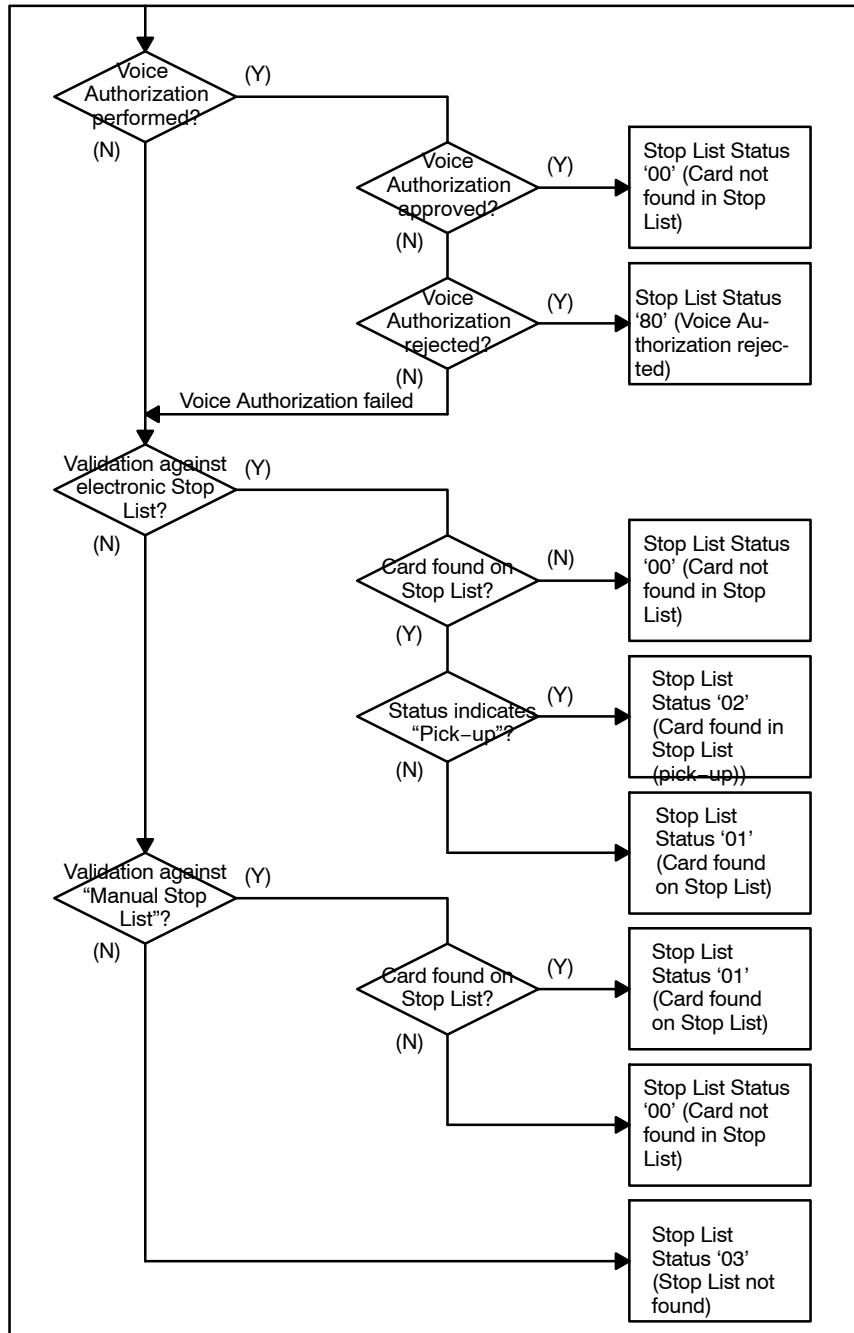


Figure 2-5.5 - Data Values for Stop List Status

2-5.3 Technology independent requirements

This section lists the common technology independent requirements for EMV, Magnetic Stripe Card, Keys Entered, Token based, ICC Prepaid and Cancellation Transactions.

EMV specific transactions are defined in sections 2-5.5 and 2-5.6 page 2-5-23 and forward. Magnetic Stripe Card specific transactions are defined in section 2-5.7 page 2-5-45 and forward. Key Entered payments are defined in section 2-5.8 page 2-5-62 and forward. Token based transactions are specified in section 2-5.9 page 2-5-72 and forward. Contactless transactions are not defined here, as the contactless kernel resides in the terminal outside the PSAM. Cancellation transactions are defined in section 2-5.10, page 2-5-84 and forward.

2-5.3.1 Transaction Processing

The Merchant Application initiates a transaction by using the appropriate Business Call.

- 2-5.3.1.1 A The terminal shall only base the flow of the transaction on the ASW1 ASW2 returned from the PSAM in the response to the different commands. The terminal shall not make any decisions on the flow based on for instance outstanding host response.

- 2-5.3.1.2 A If the terminal supports guidance for the merchant during transaction processing, the MAD-Handler shall indicate this in the data element "Info Level" which is part of the *Exchange Debit/Credit Static Information* command.

The guidance is performed by submitting a number of *Transaction State Information* commands during the transaction process. The *Transaction State Information* command gives the actual state of the transaction process. The *Transaction State Information* command can be issued from either the MAD-Handler or the PSAM.

2-5.3.2 Initialization of the Transaction

- 2-5.3.2.1 A If guidance of the merchant has been enabled, the MAD-Handler shall send a *Transaction State Information* command to the Merchant Application indicating "Waiting for card validation", when the application has been selected.

2-5.3.3 Initiate xxx Payment

Command

- 2-5.3.3.1 A The date and time ("DTHR") of the transaction shall be supported in the specified format. The same date and time shall be used as part of the printed receipt as specified in chapter 1-12 page 1-12-1, "Receipts".
- 2-5.3.3.2 A The data element "TR" (Transaction Request) shall be coded according to the Business Call initiated.

- 2-5.3.3.3 A The "Terminal Ident." (Terminal Identification) shall be coded according to ref. 20: "EMV ICC Specification".
- 2-5.3.3.4 A The data element "TT" (Transaction Type) shall be coded according to ref. 20: "EMV ICC Specification". The values can be found in section 2-15.2.164 on page 2-15-45.
- 2-5.3.3.5 A If present, the following data elements shall be part of the field "Statistics":
- Response time for previous online transaction
 - Number of time-outs
 - Number of card reader errors
 - Number of unsupported cards
 - Number of communication errors between CAD and Merchant Application
- 2-5.3.3.6 A The counters (four last bullets) shall never be reset, but be incremented each time an incident appears.
- NOTE:** If a counter reaches its maximum value (99), the terminal shall wrap the counter around to the starting value (00).
- 2-5.3.3.7 A Counters shall be reported *only* when they have been incremented.
- 2-5.3.3.8 A The field "Statistics" shall be TLV coded. The tags and format for the different data elements are defined in section 2-13.9.11 page 2-13-87.

Entering the Amount

- 2-5.3.3.9 A The length field LEN_{AMOUNTS} shall indicate the appropriate length of all the amount related fields.
- It is up to the Terminal Supplier to engage a dialog with the merchant to determine the currencies to support. The way of selecting the different currencies by the merchant is out of scope of this specification.
- NOTE:** The host or PSAM may decline a transaction if the currency is not supported.

Response

- If the PSAM requires data from the terminal (MAD-Handler), an MDOL1 (MAD-Handler Data Object List) will specify the relevant data elements in the response to the *Initiate EMV/MSC/Key Entered/Token based Payment* command.
- The Application Status Words (ASW1-ASW2) will indicate the processing status of the *Initiate EMV/MSC/Key Entered/Token based Payment* command. The possible values of ASW1-ASW2 are defined in table 2-14.143 page 2-14-136 to table 2-14.156 page 2-14-155.
- 2-5.3.3.10 A If guidance of the merchant is enabled, the MAD-Handler shall send a *Transaction State Information* command (indicating "Processing") to the Merchant Application.

2-5.3.4 EMV/MSC/Key Entered/Token based Payment

Command

- 2-5.3.4.1 A As it is the Merchant Application that is in control of the Batch Number, the MAD-Handler shall indicate the Batch Number in the *EMV/MSC/Key Entered/Token based Payment* command. The Batch Number will be part of the Financial Requests and Reversals created by the PSAM. See section 1-9.25.3 page 1-9-17 for more details concerning the Batch Number.
- 2-5.3.4.2 A If the MDOL1 (MAD-Handler Data Object List) given in the response to the *Initiate EMV/MSC/Key Entered/Token based Payment* command indicates that additional data is required, the MAD-Handler shall provide the data using the rules defined in ref. 20: "EMV ICC Specification" for Data Object Lists.

Response

The data element "CVM Status" informs the MAD-Handler whether signature is required or PIN verification has already been performed. This information is required when printing the receipt.

If the PSAM requires additional data from the terminal (MAD-Handler), an MDOL2 (MAD-Handler Data Object List) will specify the relevant data elements in the response to the *EMV/ MSC/Key Entered/Token based Payment* command.

If the PSAM has determined that an online transaction is required, the PSAM will return a complete (including APACS header) Financial Request or Authorization Request according to section 2-13 page 2-13-1.

- 2-5.3.4.3 A If an online transaction is requested, the MAD-Handler shall initiate a communication session according to ref. 27: "TAPA, Application Architecture Specification".
- 2-5.3.4.4 A If guidance of the merchant is enabled and the PSAM requires an online transaction, the MAD-Handler shall send a *Transaction State Information* command (indicating "Waiting for on-line response") to the Merchant Application.

NOTE: If the PSAM does not require an online transaction, no change in the merchant guidance shall be performed, i.e. "Waiting (processing)" is still valid.

- 2-5.3.4.5 A If guidance of the merchant is enabled and the PSAM requires an online transaction, the MAD-Handler shall send a *Transaction State Information* command (indicating "Processing") to the Merchant Application when the online response from the host is received.

2-5.3.5 Validate Data

Command

- 2-5.3.5.1 A If the MDOL2 (MAD-Handler Data Object List) given in the response to the *EMV/MSC/Key Entered/Token based Payment* command indicates that additional data is required, the MAD-Handler shall provide the data using the rules defined in ref. 20: "EMV ICC Specification" for Data Object Lists.

- 2-5.3.5.2 A If the terminal has been online, the MAD-Handler shall provide the message response received from the host (without the APACS header) as defined in section 2-13 page 2-13-1.

Response

When the PSAM has responded to the *Validate Data 2* command, the application control is returned to the MAD-Handler.

The response to the *Validate Data 2* command will conform to the format defined in section 2-14.6.3 page 2-14-59.

The Action Code (AC or AC_{PRINT}) will inform the MAD-Handler of the status of the host response in case of online transaction and the PSAM status in case of an offline transaction.

2-5.3.6 Complete xxx Payment

Command

- 2-5.3.6.1 A The data element "Transaction Status" shall be coded according to the coding defined for this data element.
- 2-5.3.6.2 A If, in case of a signature based transaction, the cardholder's signature has been verified positively, the data element "Transaction Status" shall be set to '01' (Signature accepted).

Response

When the PSAM has responded to the *Complete EMV/MSC/Key Entered Payment* command, the application control is handed back to the MAD-Handler.

If the transaction is an Original Authorization, then the response to the *Complete EMV/MSC/Key Entered Payment* command will contain a Token.

If the transaction is an Extended Authorization, then the response to the *Complete EMV/MSC Payment* command will contain a Token.

NOTE: Supplementary Authorization is described in section 2-5.9 page 2-5-72, Token Based Transactions.

- 2-5.3.6.3 A The cardholder shall be informed of the result of the transaction according to the requirement defined in section 2-4.8.1 page 2-4-10, Cardholder Display and section 2-6 page 2-6-1, Design Requirements.
- 2-5.3.6.4 A If guidance of the merchant is enabled, the MAD-Handler shall send a *Transaction State Information* command (indicating "Waiting for card") to the Merchant Application as the terminal is now ready for a new transaction.

NOTE: The result of the transaction (successful or failed) is contained in the *Transaction Completed* command to the Merchant Application.

Printing of the Receipt

- 2-5.3.6.5 A If the transaction is signature based and successful, and the PSAM requires that the cardholders signature is verified by the merchant, the MAD-Handler shall send a *Verify Signature* command to the Merchant Application.

NOTE: Whether the signature verification is required by the PSAM or not is indicated in the response to the *Exchange Debit/Credit Static information* command.

In case where the CVM is signature, the merchant can decline the transaction if he does not approve the signature.

- 2-5.3.6.6 A If the transaction is signature based and unsuccessful, the MAD-Handler shall initiate the final printing of the receipt without a field for the cardholder signature.

2-5.4 Requirements common for EMV, MSC and Key Entered Transactions

This section lists the requirements common for EMV, Magnetic Stripe Card and Keys Entered Transactions as defined in sections 2-5.5 page 2-5-23, 2-5.7 page 2-5-45 and 2-5.8 page 2-5-62 This section is structured like these three sections.

2-5.4.1 Transaction Processing

See section 2-5.3.1 page 2-5-16.

2-5.4.2 Initialization of the EMV/MSC/Key Entered Payment Transaction

- 2-5.4.2.1 A When the terminal displays the message code 'E0' ("Terminal Ready"), the terminal shall accept any order of the events (Key Pressed, Card Inserted or key entered data available).

2-5.4.3 Initiate EMV/MSC/Key Entered Payment

Command

- 2-5.4.3.1 A Whether the CVM or online/offline connection is forced by the merchant or not shall be indicated in the data element "MI" (Merchant Initiative).
- 2-5.4.3.2 A The data element POS Entry Mode shall be coded according to section 2-13.9.5 page 2-13-70.

Entering the Amount

- 2-5.4.3.3 A In cases where cashback is used, this amount (Amount, Other) shall be indicated separately in the *Initiate EMV/MSC/Key Entered Payment* command. The Transaction Type (TT) shall be set accordingly be set to '09' (Goods and services with cash disbursement) in the *Initiate EMV/MSC/Key Entered Payment* command.

NOTE: It is possible to add a cashback amount to a transaction at a late stage by specifying Amount Other in the response to the *Get Amount* command. The PSAM will then adjust the Transaction Type.

It is for the Terminal Supplier to engage in a dialogue with the merchant to determine the currencies to support. The way of

selecting the different currencies by the merchant is, with the exception of the use of Dynamic Currency Conversion, out of scope of this specification.

NOTE: Information on Dynamic Currency Conversion can be found in section 1-10.14.

- 2-5.4.3.4 C For all Original Authorization transactions, the amount may be included in the *Initiate EMV/MSC/Key Entered Payment* command.
- 2-5.4.3.5 A The terminal shall, if the amount was not included in the *Initiate xxx Payment* command, be able to respond to a *Get Amount 3* command from the PSAM before expecting the response to the *Initiate xxx Payment* command.
- 2-5.4.3.6 C For all Extended Authorization transactions, the amount may be included in the *Initiate EMV/MSC Payment* command.
- 2-5.4.3.7 A The terminal shall, if the amount was not included in the *Initiate xxx Payment* command, and the terminal has not interrupted the execution in Submit Card Reference, be able to respond to a *Get Amount 3* command from the PSAM before expecting the response to the *Initiate xxx Payment* command.

Response

See section 2-5.3.3 page 2-5-16

2-5.4.4 EMV/MSC/Key Entered Payment

Command

The implementation of a local Stop List may depend on the actual environment in which the terminal is intended to operate.

Generally, a Stop List may be implemented as

- an electronic data file with automatic look up, or
- a list with manual look up (e.g. paper based),

or alternatively

- no Stop List is implemented.

- 2-5.4.4.1 A The actual implementation of the Stop List shall not affect the value of the data element Stop List Status.
- 2-5.4.4.2 A If the Merchant Application does *not* support a Stop List, the Merchant Application Handler shall reply with "Stop List not found" in the data element "Stop List Status" in the response to the *Check Stop List* command.
- 2-5.4.4.3 A If the Merchant Application *does* support a Stop List, the Merchant Application Handler shall reply according to the coding defined for the data element "Stop List Status".

The selection value for Stop List Status, as defined by the requirements above, may be expressed by figure 2-5.5 page 2-5-15.

- 2-5.4.4.4 B When "Forced offline" is set in Merchant Initiative (MI), the Merchant Application shall request the merchant to make a Voice Authorization and enable manual entry of the Approval Code/Authorization Code.

- 2-5.4.4.5 A The result of a Voice Authorization request shall be conveyed in the response to the *Check Stop List* command.

NOTE: If the PAN is known by the merchant before it is provided in the *Check Stop List* command, the merchant may have performed the Voice Authorization previously. Alternatively, the merchant may have decided that Voice Authorization is not feasible from a business point of view.

In case of multi-application cards it may be impossible to visually read the PAN of the selected application.

- 2-5.4.4.6 A When no Approval Code/Authorization Code has been entered, the field "Approval Code" in the response to the *Check Stop List* command shall be filled with spaces.

Response

Initiation of a communication session may be initiated when the MAD-Handler Application has been selected, although the transaction may be completed offline.

2-5.4.5 Validate Data

Command

- 2-5.4.5.1 A If the terminal has *not* been online, the length field LEN_{HR} shall be set to zero.

Response

In case of a failed transaction, the Action Code from the host indicates whether retry should be performed or not.

The "Host Request" data element will be present if e.g. the PIN was rejected by the host.

- 2-5.4.5.2 A If the "Host Request" data element is present in the response to the *Validate Data 2* command, the MAD-Handler shall send the host request and continue the processing from the state where the response to *EMV/MSC/Key Entered Payment* command has just been received and continue as normal.

2-5.4.6 Complete EMV/MSC/Key Entered Payment

Command

See section 2-5.3.6 page 2-5-19

Response

- 2-5.4.6.1 A For all transactions, the MAD-Handler shall send a *Transaction Completed* command to the Merchant Application. The merchant can then decide whether the goods or services shall be handed over or not.

Printing of the receipt

The layout of the receipts and the information printed depends on the transaction result and the type of CVM used as stated in section 1-12 page 1-12-1, Receipts.

2-5.5 EMV Card Transactions

2-5.5.1 Transaction Processing

The terminal must select the card application that is to be used for a particular transaction as defined in section 1-14.3 page 1-14-3. If the EMV application is selected, then the payment transaction is conducted according to this specification.

Figures 2-5.6 page 2-5-32 to 2-5.11 page 2-5-42 provides examples of typical message flows for successful EMV transactions. For a description of the handlers depicted in the figures, refer to ref. 27: "TAPA, Application Architecture Specification".

2-5.5.2 Initialization of the EMV Debit/Credit Payment Transaction

- 2-5.5.2.1 A If the response to the *Get Event* command indicates that a card has been inserted, the MAD-Handler shall send a *Transaction State Information* command (if enabled) to the Merchant Application indicating "Waiting for application Selection".
- 2-5.5.2.2 A As soon as the MAD-Handler has been informed that an ICC was inserted, the MAD-Handler shall perform application selection according to section 1-14.3 page 1-14-3 ICC Application Selection.

2-5.5.3 Initiate EMV Payment

The boxes labeled "EMV1" contained in figure 2-5.6 page 2-5-32 to figure 2-5.11 page 2-5-42 covers the following actions according to ref. 20: "EMV ICC Specification":

- Initiate Application Processing
- Reading of Application Data
- Offline Data Authentication
- Processing Restrictions
- Cardholder Verification

These functions are performed by the PSAM.

Command

By issuing an *Initiate EMV Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the User Interface Handler and the Merchant Application Handler.

- 2-5.5.3.1 A The *Initiate EMV Payment 2* command shall conform to the format defined in section 2-14.6.1 page 2-14-54.
- 2-5.5.3.2 A The data element "Card Data Source" shall be set to '00' indicating contact based EMV.
- 2-5.5.3.3 A Both the length of the AID (LEN_{AID}) and the full Application ID (AID_{EMV}) received in the response to the *Select* command sent to the ICC shall be given in the command.

- 2-5.5.3.4 B The FCI (File Control Information) returned by a successful selection of the ADF shall be part of the *Initiate EMV Payment* command, if the total length of the *Initiate EMV Payment* command does not exceed the maximum limit.

NOTE: Since the maximum value of the data element L_C is 255 bytes, the maximum value of the data element L_{DATA} is $255 + 6 = 261$.

NOTE: FCI shall include all bytes starting with '6F' (FCI template). The Status Words SW1-SW2 shall not be included.

- 2-5.5.3.5 A If the total length of the *Initiate EMV Payment* exceeds the limit defined in requirement 2-5.5.3.4, the field "FCI" shall be omitted from the *Initiate EMV Payment* command and the value of LEN_{FCI} is set to '00'.

If the FCI is omitted in the *Initiate EMV Payment* command, the PSAM will send a *Repeat Last ICC Response* command to the Card Handler to obtain the FCI.

Entering the Amount

For the Purchase/Refund/Original Authorization transaction, the amount may be present before the *Initiate EMV Payment* command is issued. If the amount is not available in the *Initiate EMV Payment* command, the PSAM will obtain the amount from the Merchant Application at the appropriate time.

NOTE: The *Get Amount* command will be issued to obtain the amount. Depending of the actual EMV card and the response to the *Get Amount* command dual issues of this command may occur as described in section 2-8.4.2 page 2-8-3.

If guidance of the merchant has been enabled, the PSAM will send a *Transaction State Information* command to the Merchant Application indicating "Waiting for PIN and amount", when PIN entry is initiated.

Account Type

- 2-5.5.3.6 A For terminals where both terminal and PSAM support Service Pack No. 2, the Account Type shall be inserted as the final data element. See section 2-15.2.1 on page 2-15-2 for further details concerning Account Type.

Card Reference

For an Extended Authorization transaction, the PSAM will issue a *Submit Card Reference* command.

- 2-5.5.3.7 A If the terminal (Merchant Handler) wants to interrupt the Extended Authorization transaction deliberately, i.e. because the transaction is performed with the only purpose of creating a card reference, the terminal shall return a specific Response Code, RC = 'FFFD' (Transaction interrupt request) in the response to the *Submit Card Reference* command.

PIN Entry

If PIN entry is required as the CVM, the PIN entry must be performed according to ref. 27: "TAPA, Application Architecture

Specification” and requirements described in this specification.

Response

When the PSAM has responded to the *Initiate EMV Payment* command, the application control is returned to the MAD-Handler.

The response to the *Initiate EMV Payment 2* command will conform to the format defined in section 2-14.6.1 page 2-14-54.

The Card official name (Card Name), Application Effective Date (DATE_{EFFECTIVE}), Application PAN Sequence Number (PAN_{SEQUENCE}) and the Primary Account Number (PAN), all related to the printing of the receipt, will be delivered in the response.

MDOL1 will typically contain data elements which are requested by the ICC (indicated in the Card Risk Management Data Object List (CDOL1)) and are not already present in the PSAM.

2-5.5.4 EMV Payment

The boxes labeled “EMV2” contained in figure 2-5.6 page 2-5-32 to figure 2-5.11 page 2-5-42 covers the following actions according to ref. 20: “EMV ICC Specification”:

- Terminal Action Analysis
- Card Action Analysis

Terminal Action Analysis is performed by the PSAM and Card Action Analysis is performed by the ICC-

Command

By issuing an *EMV Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

- 2-5.5.4.1 A The *EMV Payment* command shall conform to the format defined in section 2-14.6.2 page 2-14-57.

For both online and offline transactions, the PSAM will provide the necessary card data to the Merchant Application Handler for performing a Stop List check.

Response

When the PSAM has responded to the *EMV Payment* command, the application control is returned to the MAD-Handler.

The response to the *EMV Payment* command will conform to the format defined in section 2-14.6.2 page 2-14-57.

Application Transaction Counter (ATC), related to the printing of the receipt, is part of the response as well.

MDOL2 will typically contain data elements which are requested by the ICC (indicated in the Card Risk Management Data Object List (CDOL2)) and are not already present in the PSAM.

NOTE: If the transaction is offline approved, i.e. the card returns a Transaction Certificate (TC) on the first EMV related *Generate AC* command, no request is returned.

- 2-5.5.4.2 A The ATC to be printed on the receipt shall be taken from the response to the *EMV Payment* command.

2-5.5.5 **Validate Data**

The boxes labeled "EMV3" contained in figure 2-5.6 page 2-5-32 to figure 2-5.11 page 2-5-42 covers the following actions according to ref. 20: "EMV ICC Specification":

- Issuer Authentication
- Issuer-to-Card Script Processing

These functions are performed by the PSAM.

NOTE: The *Validate Data 2* command may consist of one or two segments depending of the amount of data.

Command

By issuing a *Validate Data 2* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

NOTE: The *Validate Data 2* command may consist of one or two segments depending of the amount of data.

- 2-5.5.5.1 A The *Validate Data 2* command shall conform to the format defined in section 2-14.6.3.

Response

Although the Application Status Words (ASW1- ASW2) indicates declined (e.g. '1221' incorrect PIN), the terminal shall continue as stated in requirement 2-5.4.5.2 page 2-5-22.

- 2-5.5.5.2 C If the response to the *Validate Data 2* command does not contain a Host Request, the *ICC Power-Off* command may be sent to the Card Handler.

Issuer Scripts to a Card

Scripts may be used to change parameters in an ICC according to ref. 20: "EMV ICC Specification".

Scripts may be sent to the ICC, inserted in the terminal, when the terminal is on-line.

Scripts are forwarded by the acquirer on behalf of the Issuer.

If the Issuer recognizes the ICC, inserted in the terminal, as an ICC which needs to have some parameters changed, the acquirer will send an Issuer Script for the ICC. The PSAM will handle script processing.

2-5.5.6 Complete EMV Payment

The boxes labeled “EMV4” contained in figure 2-5.6 page 2-5-32 to figure 2-5.11 page 2-5-42 covers the following actions according to ref. 20: “EMV ICC Specification”:

- Completion

This function is performed by the PSAM.

Command

By issuing a *Complete EMV Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the Data Store Handler (e.g. if an offline transaction is performed) and the Merchant Application Handler if logging of transaction data is enabled.

- 2-5.5.6.1 A The *Complete EMV Payment* command shall conform to the format defined in section 2-14.6.4 page 2-14-65.

Response

The response to the *Complete EMV Payment* command will conform to the format defined in section 2-14.6.4 page 2-14-65.

2-5.5.7 EMV-related Data Elements

EMV-related data elements, which are stored in the terminal and PSAM, fall into one of the following classifications:

- Data elements which are terminal-specific and therefore reside in the terminal. These data elements are normally conveyed to the PSAM during configuration or by use of MDOL data (MAD-Handler Data Object List data).
- Data elements that must be update-able by the issuer/acquirer and therefore reside in the PSAM (indicated as mandatory (M) in table 2-5.2 page 2-5-28).
- Data elements that are conveyed in messages and are therefore stored and maintained inside the PSAM. These data elements are not indicated in table 2-5.2 page 2-5-28).
- Data elements that may reside in either the terminal, PSAM or at the acquirer (indicated as optional (O) in table 2-5.2 page 2-5-28)

Data elements listed in table 2-5.2 page 2-5-28 are all defined in ref. 20: “EMV ICC Specification”.

NOTE: The data elements listed in *italics* in table 2-5.2 page 2-5-28 may all be included as part of the Processing Option Data Object List (PDOL).

All TLV data elements that originate from the card are temporarily stored in the PSAM.

Table 2-5.2 - Storage of Data Elements

Data Element	Reside in PSAM		Reside in Terminal	Update able (Acquirer/Issuer)	Comments
	M	O			
<i>Acquirer Identifier</i>		☐			Added by the acquirer host
<i>Additional Terminal Capabilities</i>			Origin		Conveyed to PSAM ¹⁾
<i>Amount, Authorized (Binary)</i>	☐		Origin		From Merchant Application ²⁾
<i>Amount, Other (Binary)</i>	☐		Origin		From Merchant Application ²⁾
<i>Amount, Reference Currency</i>		☐			From Merchant Application
<i>Application Identifier (AID)</i>	☐			☐	
<i>Application Version Number</i>	☐				
<i>Authorization Response Code</i>	☐			☐	
<i>Cardholder Verification Method Results</i>	☐				
<i>Certification Authority Public Key</i>	☐			☐	Required if SDA/DDA or offline PIN encipherment
<i>Certification Authority Public Key Index</i>	☐			☐	Required if SDA/DDA or offline PIN encipherment
<i>Command Template</i>	☐				
<i>Interface Device Serial Number</i>			Origin		Conveyed to PSAM ¹⁾
<i>Merchant Category Code</i>	☐				
<i>Merchant Identifier</i>	☐				
<i>Point-of-Service Entry Mode</i>			Origin		Conveyed to PSAM ²⁾
<i>Terminal Capabilities</i>			Origin		Conveyed to PSAM ¹⁾
<i>Terminal Country Code</i>	☐				
<i>Terminal Floor Limit</i>	☐			☐	
<i>Terminal Identification</i>			Origin		Conveyed to PSAM ¹⁾
<i>Terminal Risk Management Data</i>	☐			☐	
<i>Terminal Type</i>			Origin		Conveyed to PSAM ¹⁾
<i>Terminal Verification Results</i>	☐				
<i>Transaction Certificate Hash Value</i>	☐				
<i>Transaction Currency Code</i>	☐		Origin		From Merchant Application ²⁾
<i>Transaction Currency Exponent</i>	☐		Origin		From Merchant Application ²⁾
<i>Transaction Date</i>		☐	Origin	☐	
<i>Transaction Personal Identification Number Data</i>	☐				From PIN Pad (User Interface)
<i>Transaction Reference Currency Code</i>	☐				
<i>Transaction Reference Currency Exponent</i>	☐				
<i>Transaction Sequence Number</i>	☐				
<i>Transaction Status Information</i>	☐				
<i>Transaction Time</i>			Origin		
<i>Transaction Type</i>	☐				Conveyed to PSAM ²⁾
<i>Unpredictable Number</i>	☐				

NOTES: 1) Conveyed in the *Exchange Debit/Credit Static Information* command.
2) Conveyed in the *Initiate EMV Payment* command.

2-5.6 Optimizing the Transaction Time, EMV

2-5.6.1 Introduction

In order to speed up the EMV transaction flow when PIN is used as CVM, two different functions are introduced. Depending on the actual card, the PSAM will decide whether the basic EMV rules apply or if PIN entry may be initiated earlier. The functions are described in details below.

2-5.6.2 Accelerated PIN Entry

The PSAM may perform the Accelerated PIN Entry, APE, flow under certain conditions in order to allow PIN entry earlier than the original flow allows.

When Accelerated PIN Entry is used, the sequence of commands issued by the PSAM is different from the original flow. The major difference is that the commands *Get KCV* and *Initiate PIN Entry* are issued by the PSAM as soon as possible.

The Accelerated PIN Entry exists in two versions: APE and DAPE, Dankort APE, both of which are described in table 2-5.3 page 2-5-30.

DAPE has been introduced in order to speed up the transaction flow when using the national debit card Dankort/VisaDankort. For all other cards APE have been introduced.

The proprietary handling of Dankort/VisaDankort makes it possible to enable PIN entry earlier than otherwise allowed for in EMV. This makes DAPE possible.

However, for all other cards, EMV rules for CVM selection must be observed, i.e. the handling of the Cardholder Verification Method List read from the card.

In the original flow, the CVM is determined after all *Read Records* commands have been performed, and only after the transaction amount is known to the PSAM. If the result of the CVM selection process is that PIN is needed, the commands *Get KCV* and *Initiate PIN Entry* are issued by the PSAM.

In APE, the CVM is determined as soon as all the *Read Records* commands are performed and it is verified that the transaction amount is not needed in order to start PIN Entry. This enables the PSAM to issue the commands *Get KCV* and *Initiate PIN Entry* before the transaction amount is known.

In DAPE, the CVM selection process is based on advance knowledge of which card scheme is being used to perform the transaction. In the *Initiate EMV Payment* command the relevant information needed to determine the national card scheme is contained in the File Control Information (FCI) returned from the Final Select. This makes it possible to identify the national debit card scheme Dankort/VisaDankort and hence issue *Get KCV* and *Initiate PIN Entry* commands before *Get Processing Options* command.

APE and DAPE is controlled by Nets. The functionality is by default enabled.

If needed, it can be disabled by the Host system for one or more or all AIDs. It is only possible to disable APE and DAPE

for all terminals related to the same ME_{NUMBER}. Enabling/disabling for individual terminals is not possible.

NOTE: Accelerated PIN Entry (APE) and Dankort Accelerated PIN Entry (DAPE) are applicable for EMV transactions only.

Table 2-5.3 - Accelerated PIN Entry Vs. Original Flow (Example - Dankort - Online Purchase)

EMV Command Flow			
Terminal	PSAM		
	Original Flow	Accelerated PIN Entry (APE)	Dankort Accelerated PIN Entry (DAPE)
Initiate Payment ⓘ			
	Get Processing Options	Get Processing Options	Get KCV ¹⁾
	Read Record	Read Record	Initiate PIN Entry
	Read Record	Read Record	Get Processing Options
	◆	◆	Read Record
	Get Amount	Get KCV ¹⁾	Read Record
	Get KCV ¹⁾	Initiate PIN Entry	◆
	Initiate PIN Entry	Get Amount	Get Amount
	Confirm Amount	Confirm Amount	Confirm Amount
	Get PIN	Get PIN	Get PIN
Terminate PIN Entry	Terminate PIN Entry	Terminate PIN Entry	
Initiate Payment Ⓢ			
Payment ⓘ			
	Check Stop List ²⁾	Check Stop List ²⁾	Check Stop List ²⁾
	1st Generate AC	1st Generate AC	1st Generate AC
Payment Ⓢ			
Validate Data ⓘ			
	2nd Generate AC	2nd Generate AC	2nd Generate AC
Validate Data Ⓢ			
Complete Payment ⓘ			
	Add File Record	Add File Record	Add File Record
Complete Payment Ⓢ			

Legend:

ⓘ = Command, Ⓢ Response, ◆ Additional Read Records may be issued.

1) Get KCV is not issued if the PTS synchronization flow is performed between the PED and the PSAM.

2) The Check Stop List command is only issued if forced offline, to allow for entry of voice authorization data.

2-5.6.3 Release of the ICC

When the terminal has received the response to the *Validate Data 2* command, the terminal may send the *ICC Power-off* command to the Card Handler and indicate in the Cardholder Display that the card may be retained (“Remove Card”/“Husk kort”).

At this time all communication with the ICC is finished, but the final result of the transaction is not determined at this point i.e. neither the display text “Approved”/“Godkendt” nor an audio signal indicating approved may be initiated at this time.

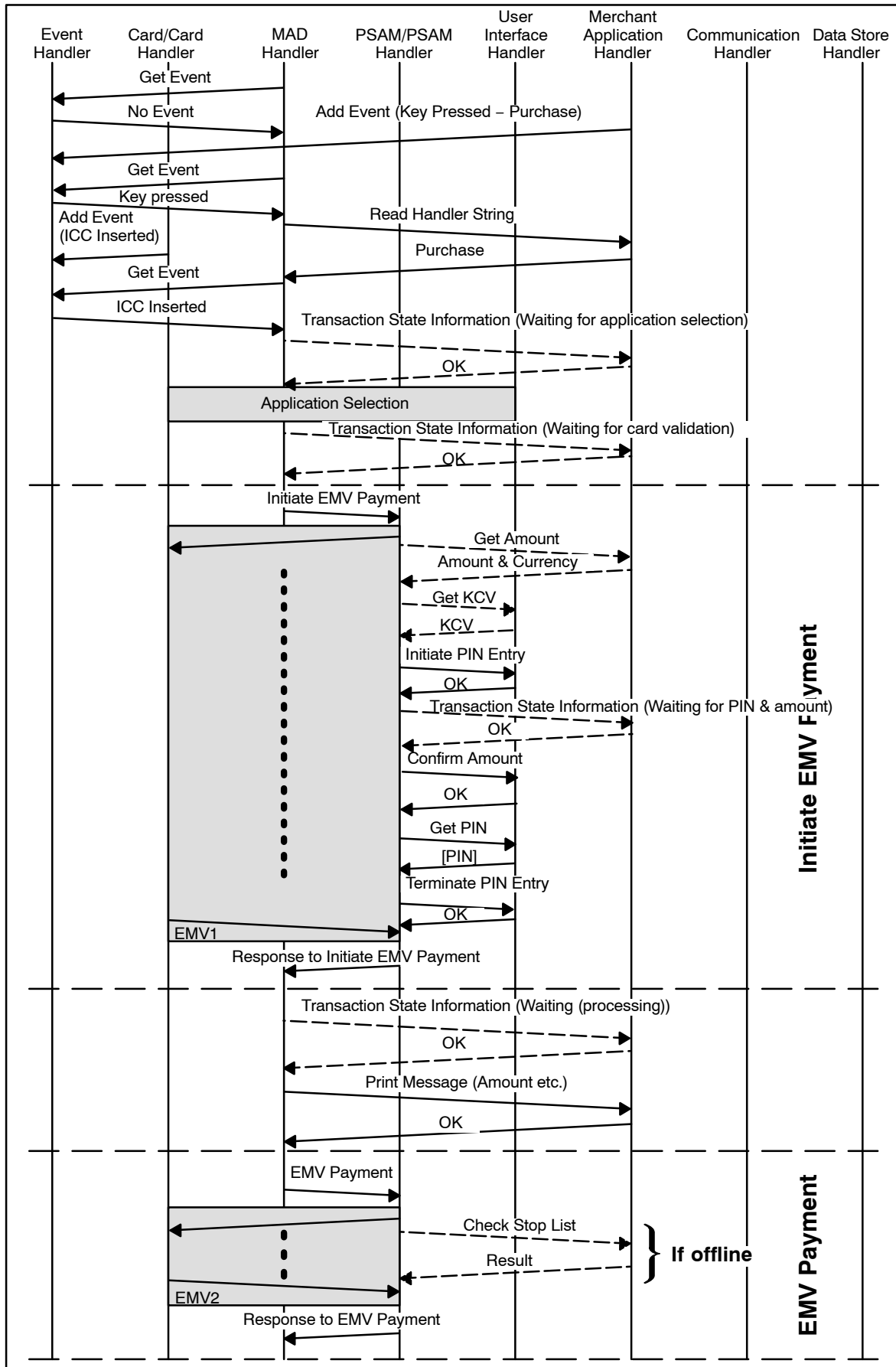


Figure 2-5.6 - EMV Transaction (Purchase - PIN)

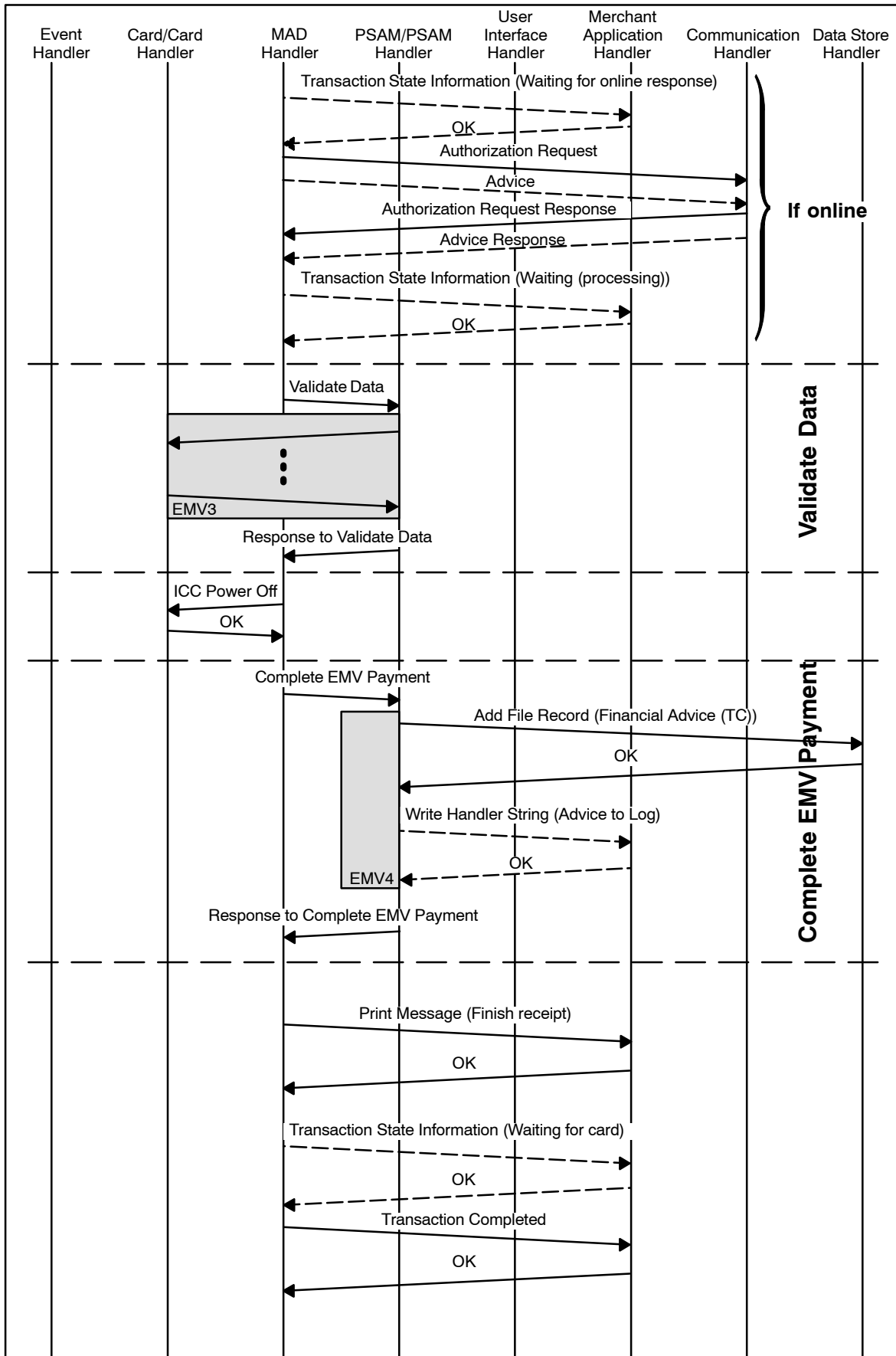


Figure 2-5.6 - EMV Transaction (Purchase - PIN) (concluded)

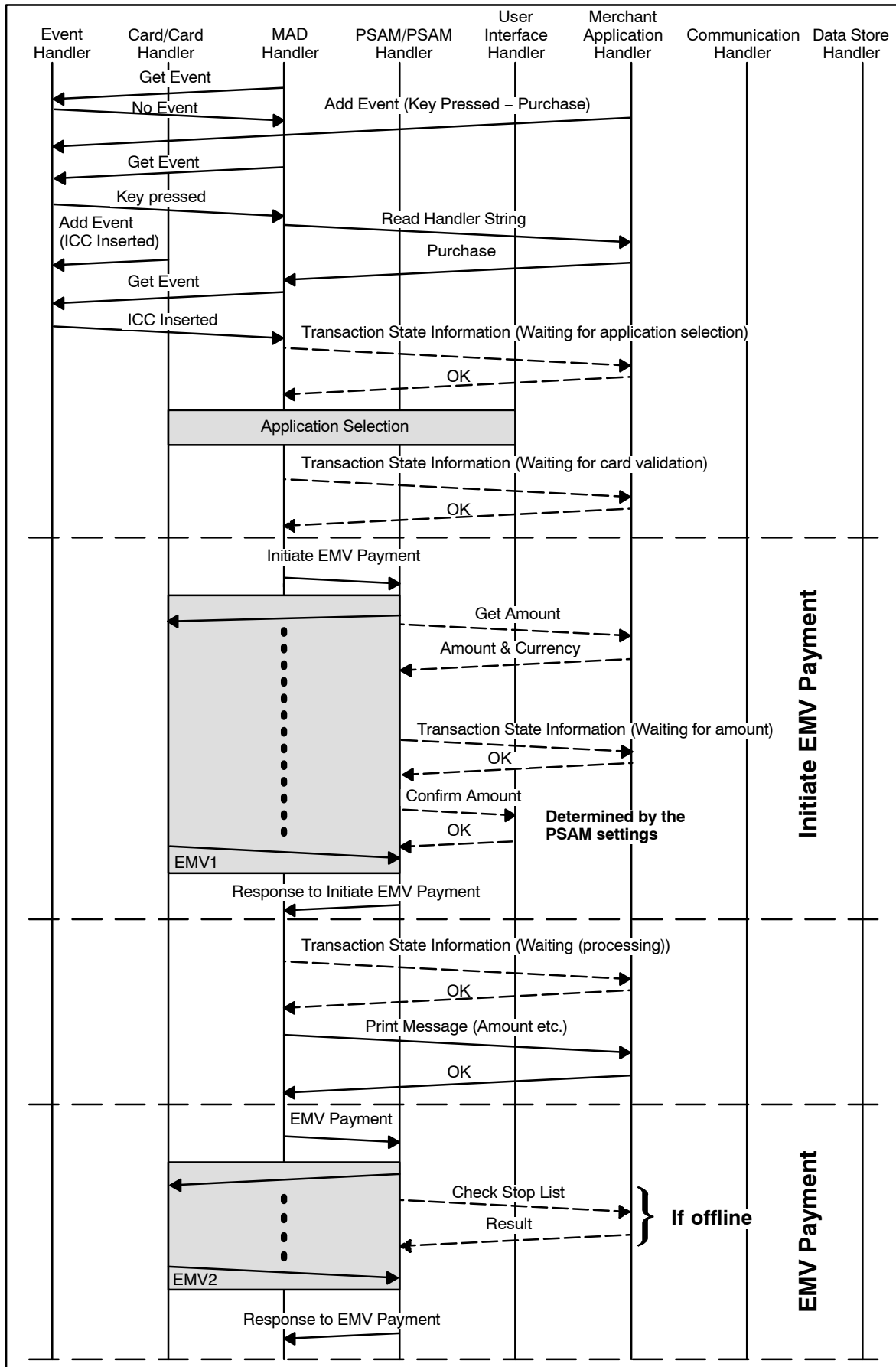


Figure 2-5.7 - EMV Transaction (Purchase - Signature)

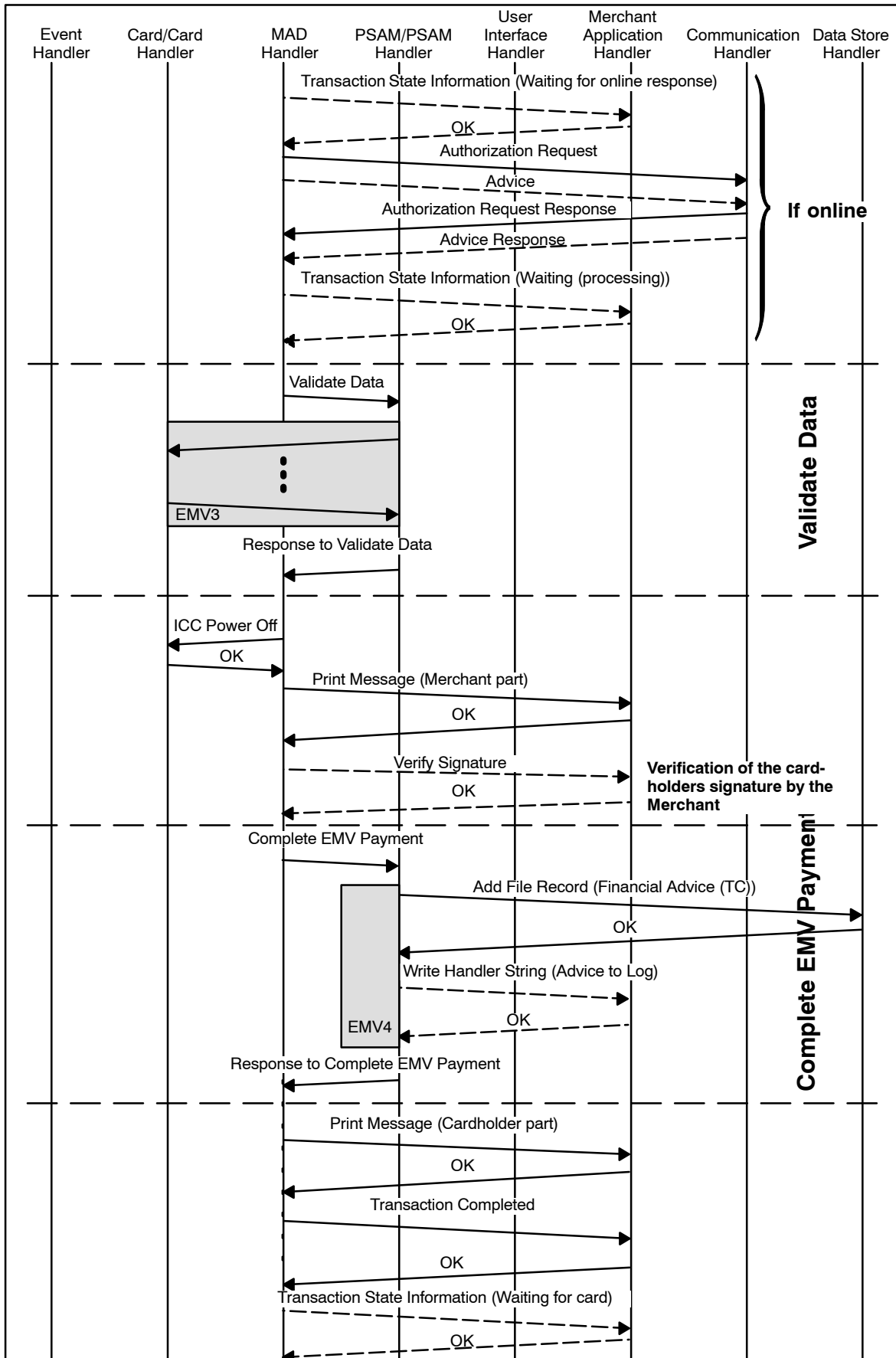


Figure 2-5.7 - EMV Transaction (Purchase - Signature) (concluded)

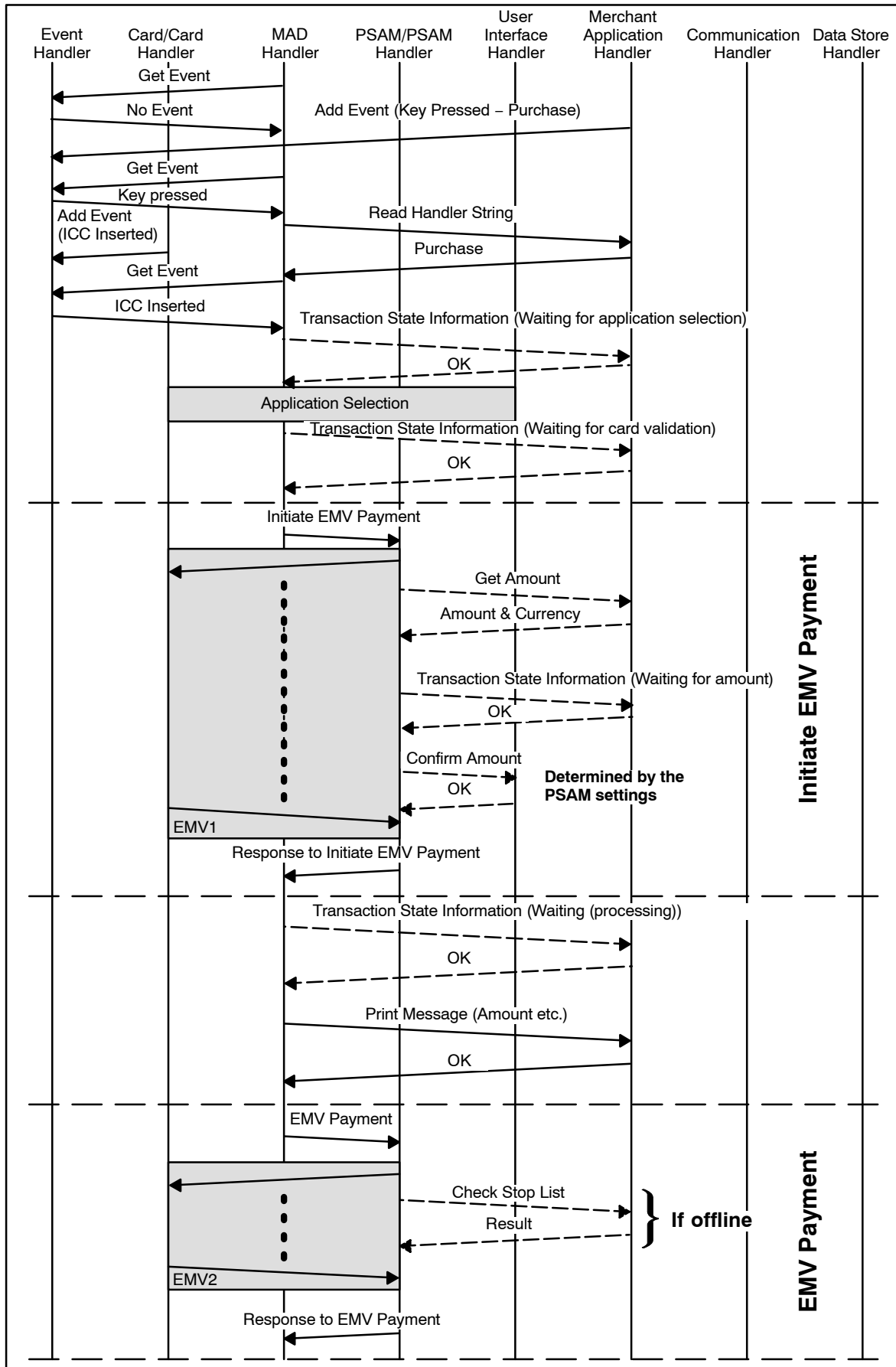


Figure 2-5.8 - EMV Transaction (Purchase - No CVM)

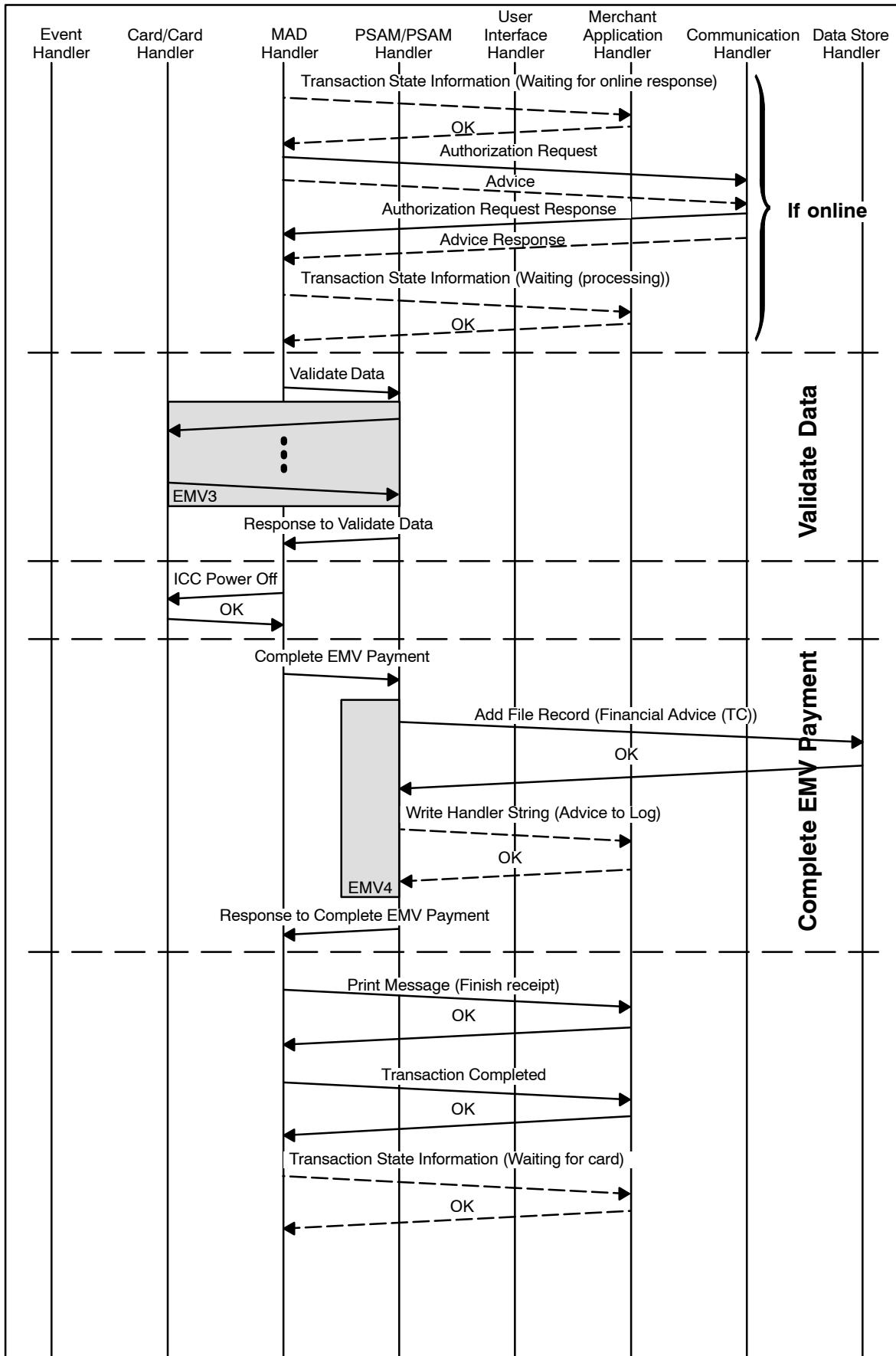


Figure 2-5.8 - EMV Transaction (Purchase - No CVM) (concluded)

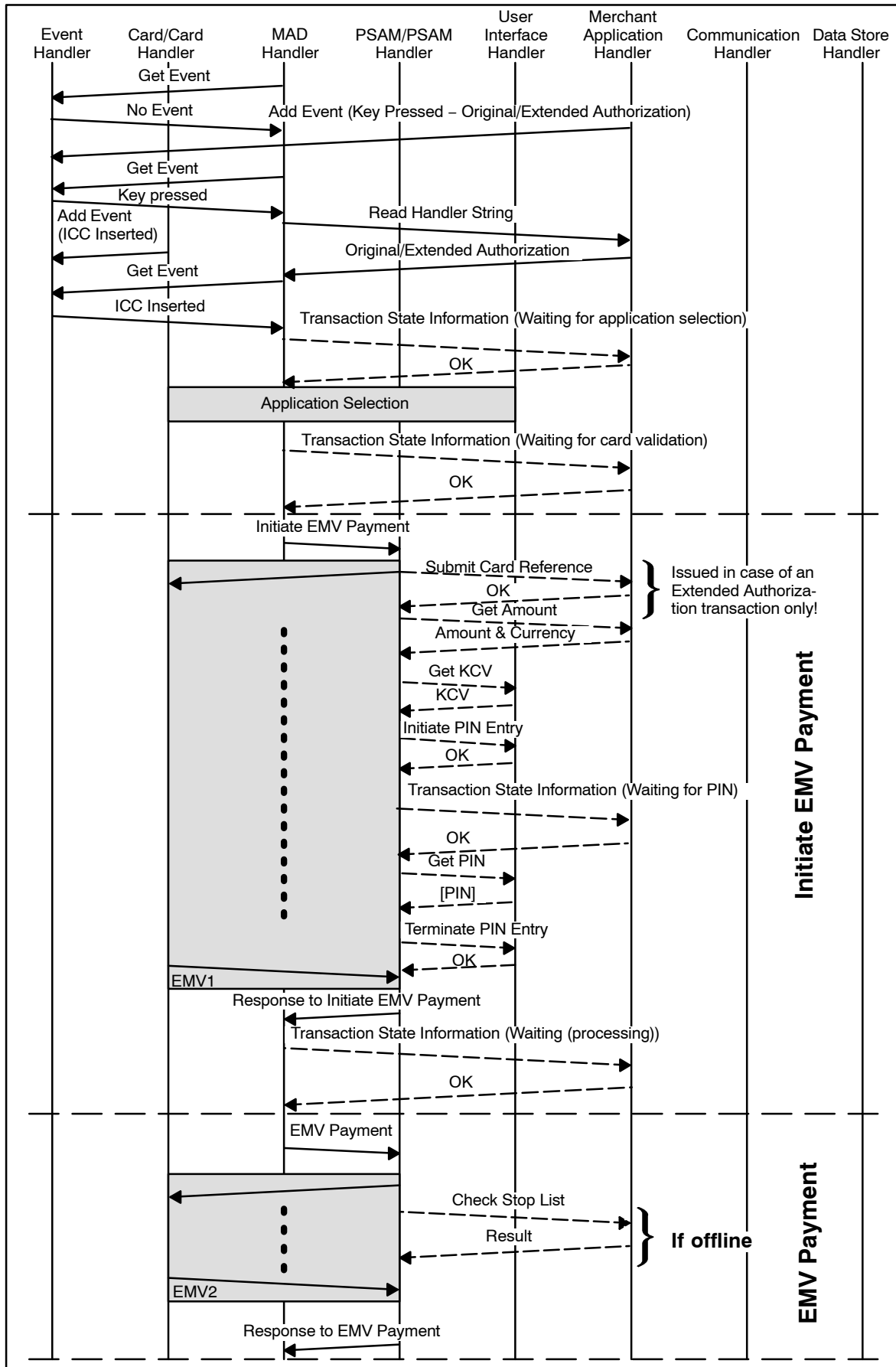


Figure 2-5.9 - EMV Transaction (Original/Extended Authorization - PIN/No CVM)

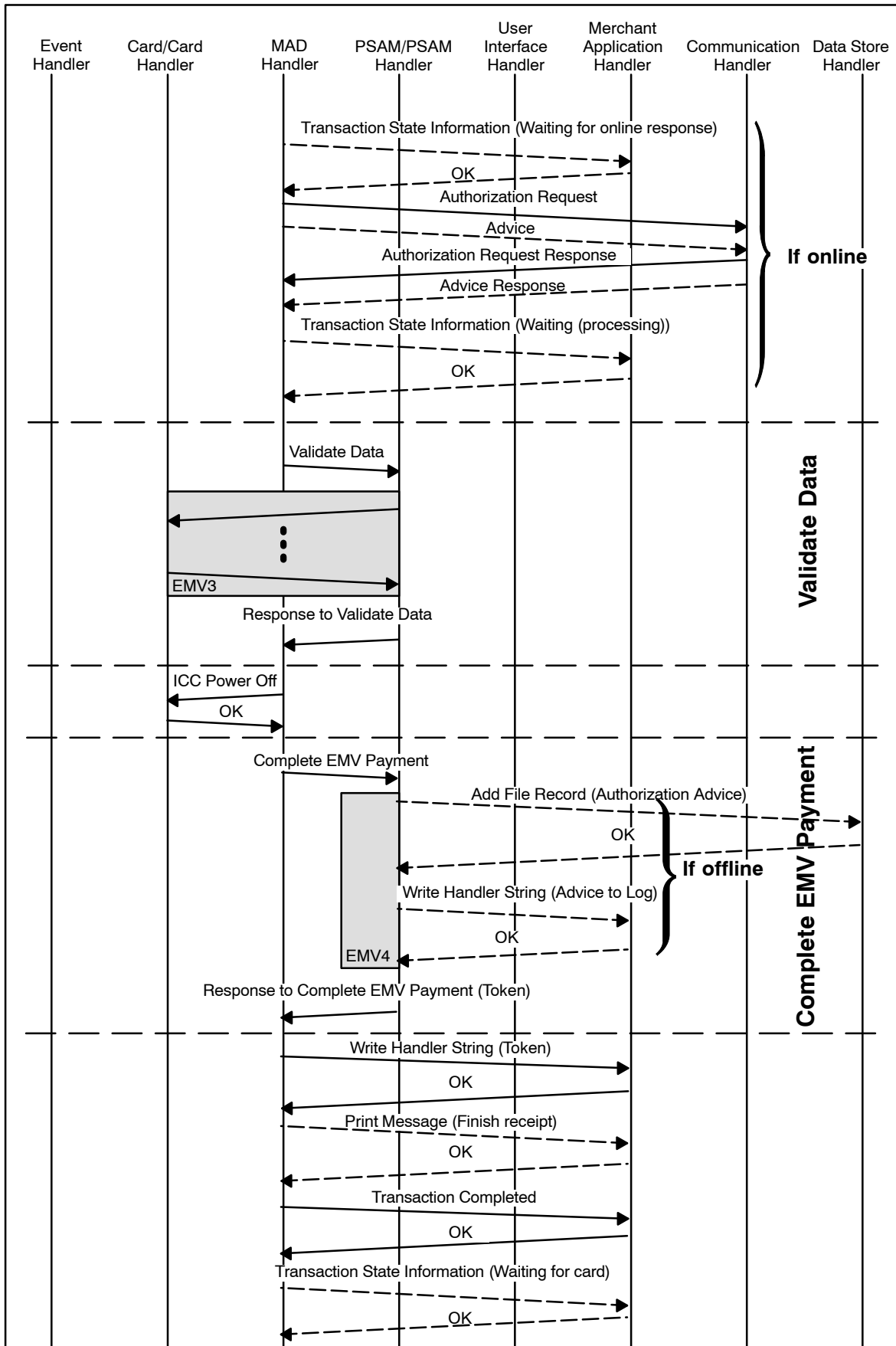


Figure 2-5.9 - EMV Transaction (Original/Extended Authorization - PIN/No CVM) (concluded)

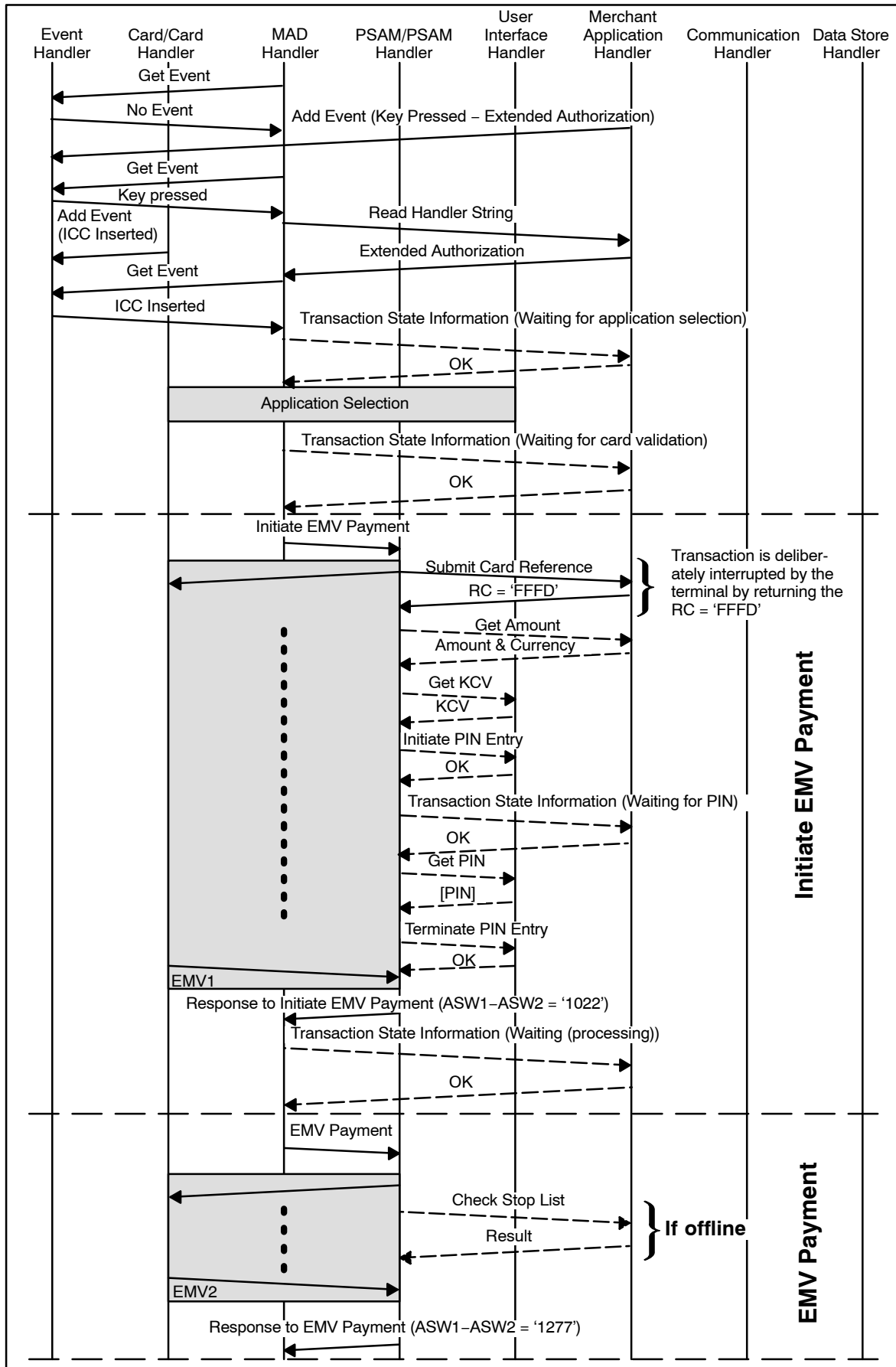


Figure 2-5.10 - EMV Transaction (Extended Auth. - Interrupted - PIN/No CVM)

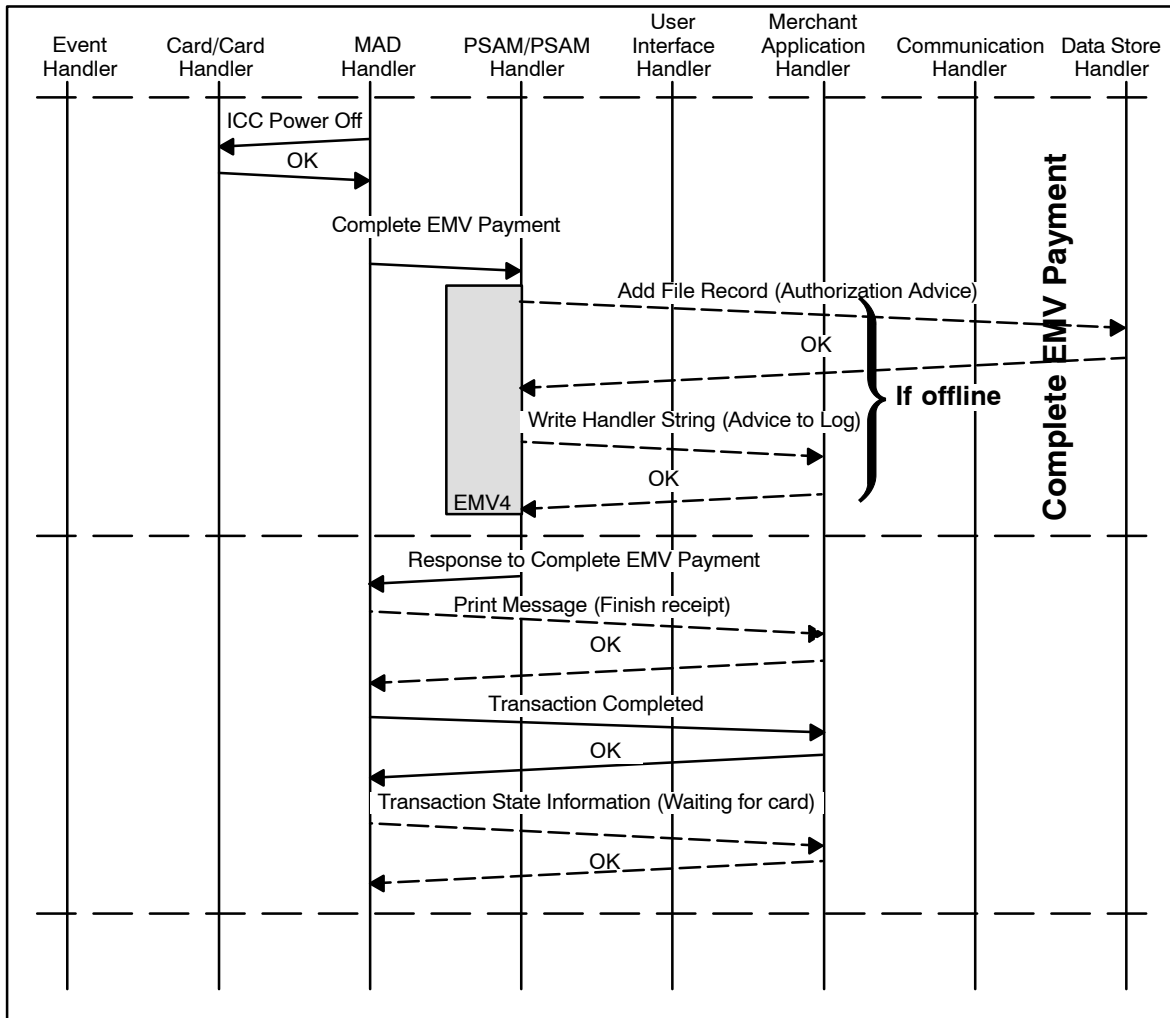


Figure 2-5.10 - EMV Transaction (Extended Authorization - Interrupted - PIN/No CVM) (concluded)

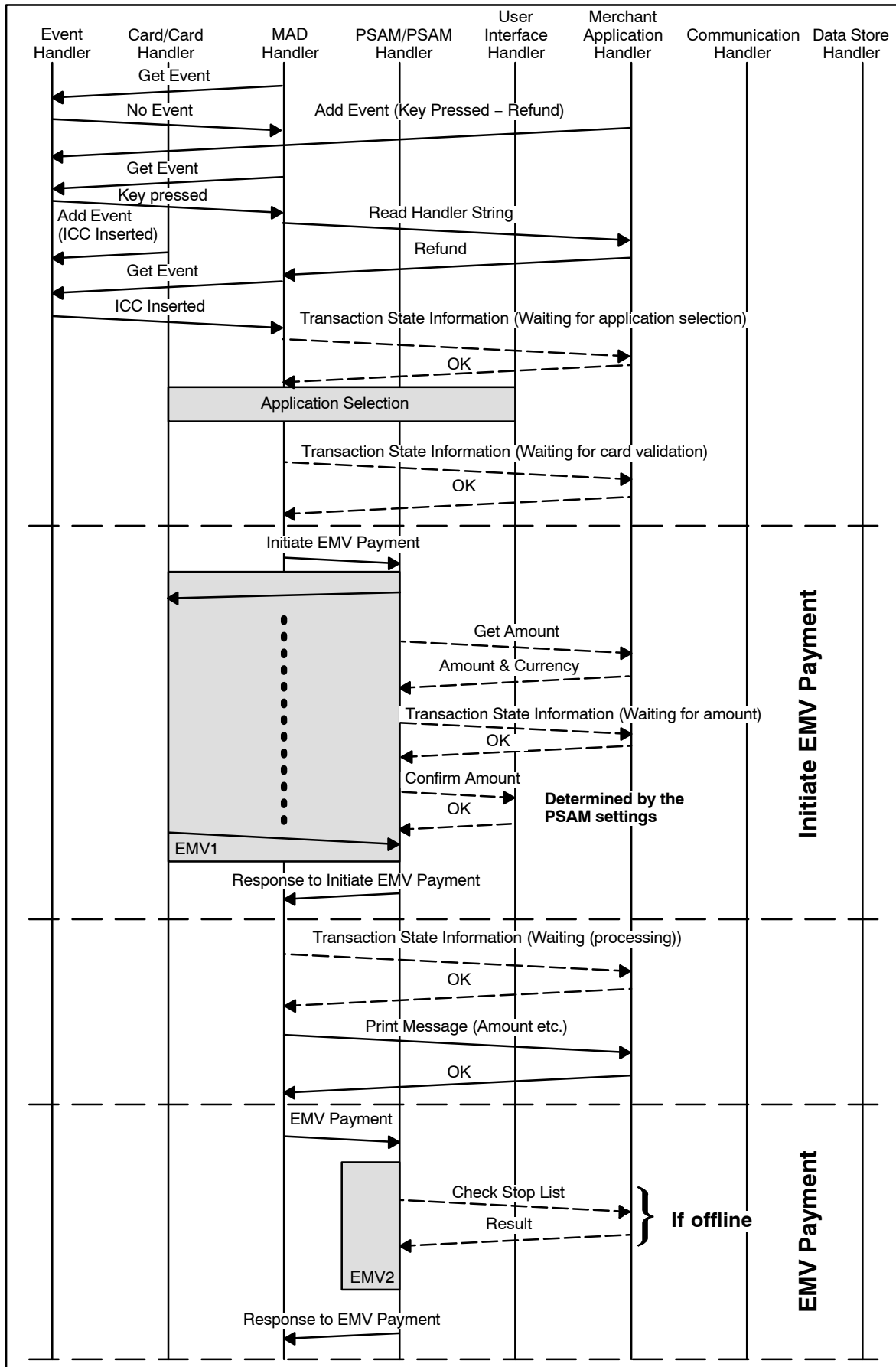


Figure 2-5.11 - EMV Transaction (Refund - Signature)

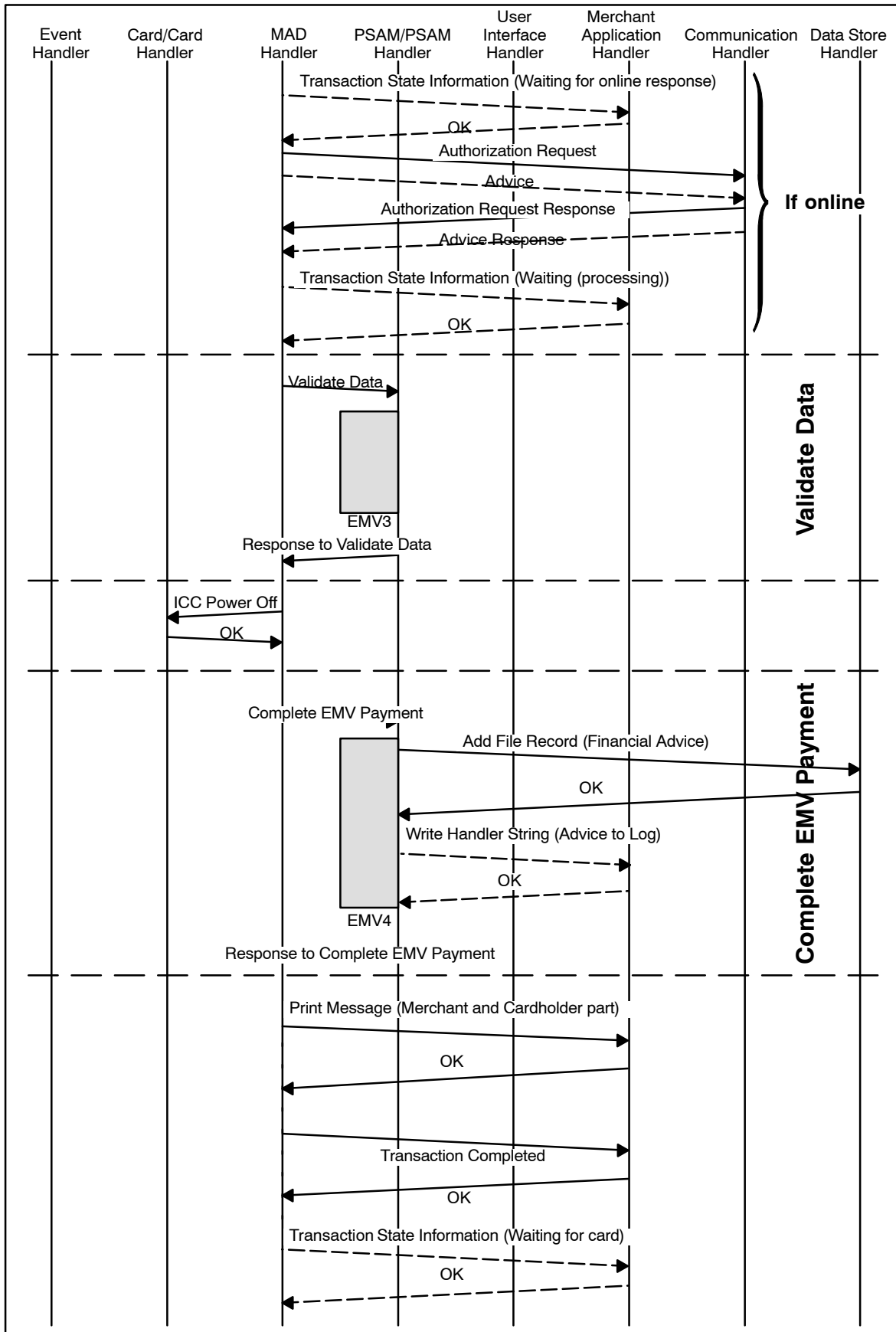


Figure 2-5.11 - EMV Transaction (Refund - Signature) (concluded)

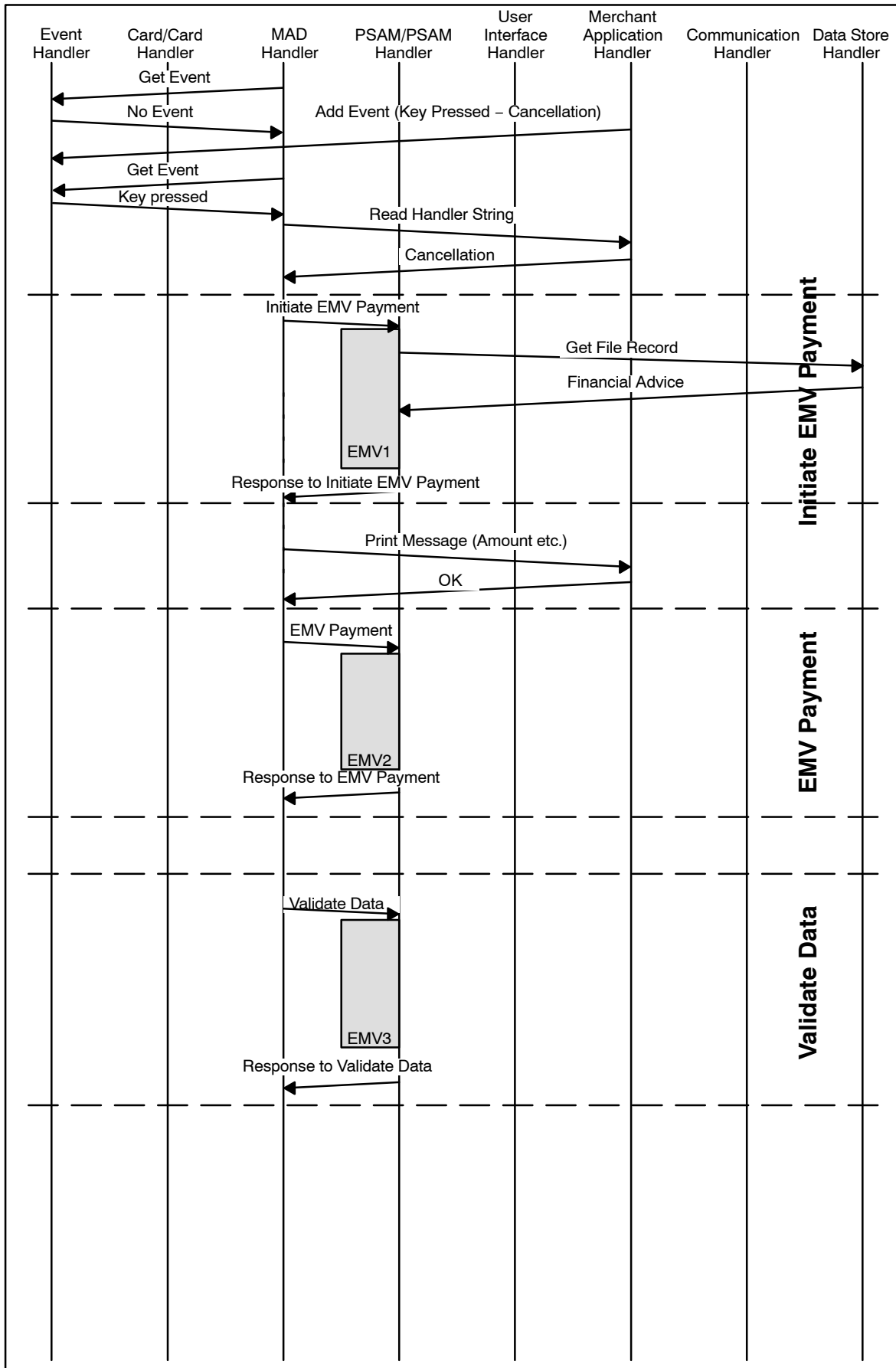


Figure 2-5.12 - EMV Transaction (Cancellation)

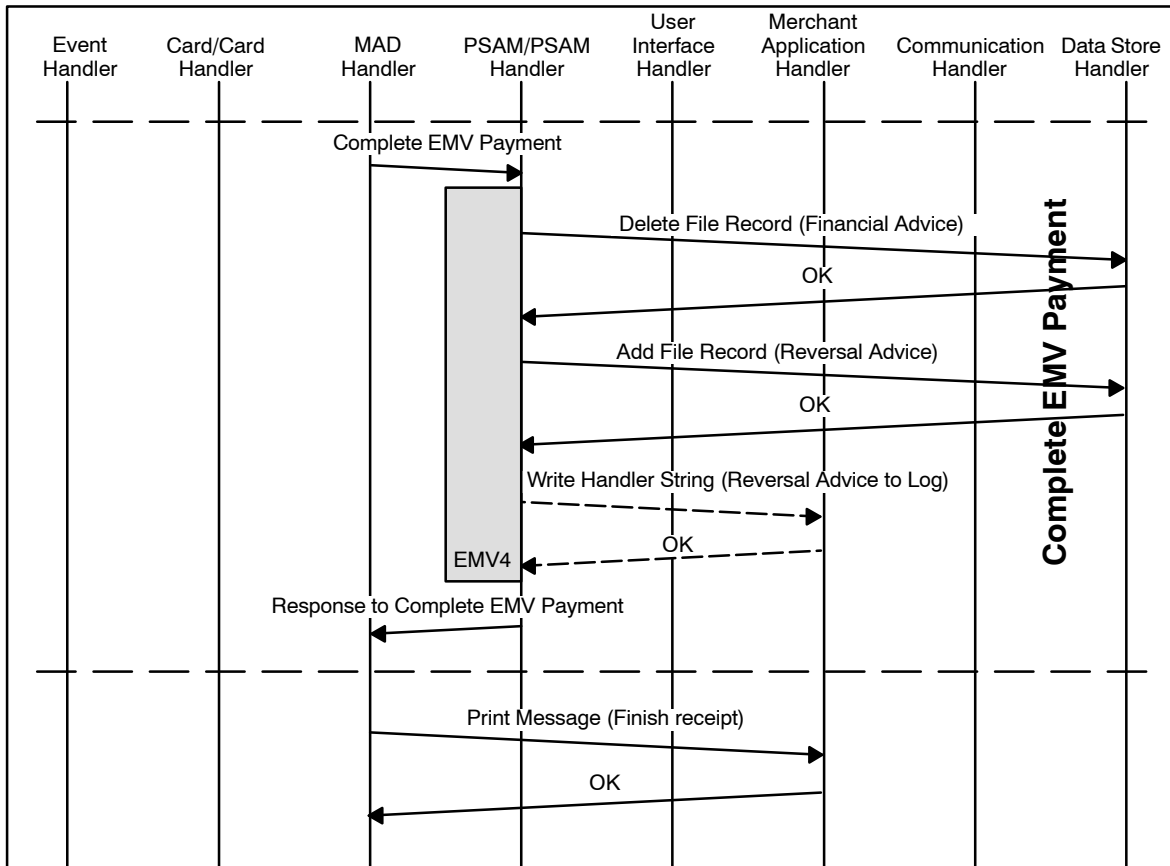


Figure 2-5.6 - EMV Transaction (Cancellation) (concluded)

2-5.7 Magnetic Stripe Card Transactions

2-5.7.1 Transaction Processing

Figures 2-5.13 page 2-5-49 to 2-5.17 page 2-5-57 provides examples of typical message flows for successful MSC transactions. For a description of the handlers depicted in the figures, refer to ref. 27: "TAPA, Application Architecture Specification".

2-5.7.2 Initialization of the MSC Debit/Credit Payment Transaction

- 2-5.7.2.1 A If the response to the *Get Event* command indicates that a card has been swiped, the MAD-Handler shall send a *Transaction State Information* command (if enabled) to the Merchant Application indicating "Waiting for Application Selection".
- 2-5.7.2.2 A As soon as the MAD-Handler has been informed that a MSC was swiped, the MAD-Handler shall perform application selection according to section 1-14.3.4 page 1-14-11 "MSC Application Selection".
- 2-5.7.2.3 C When the MAD-Handler application has been selected, the address information (e.g. the telephone number etc.) to use when establishing the online connection may be identified.

NOTE: For MSC based transactions, the call may be initiated when the application has been identified.

2-5.7.3 Initiate MSC Payment

Command

By issuing an *Initiate MSC Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the User Interface Handler and the Merchant Application Handler.

- 2-5.7.3.1 A The *Initiate MSC Payment 2* command shall conform to the format defined in section 2-14.6.5 page 2-14-66.
- 2-5.7.3.2 A The data element "Card Data Source" shall be set to '01' indicating MSC.
- 2-5.7.3.3 A The track 2 or track 3 data read by the *Read Magnetic Stripe* command shall be conveyed in the data element "TRACK2 DATA".

Entering the Amount

For the Purchase/Refund/Original Authorization transaction, the amount may be present before the *Initiate MSC Payment* command is issued. If the amount is not available in the *Initiate MSC Payment* command, the PSAM will obtain the amount from the Merchant Application at the appropriate time.

Account Type

- 2-5.7.3.4 A The Account Type shall be inserted as the final data element. See section 2-15.2.1 page 2-15-2 for further details concerning Account Type.

Card Reference

For an Extended Authorization transaction, the PSAM will issue a *Submit Card Reference* command.

- 2-5.7.3.5 A If the terminal (Merchant Handler) wants to interrupt the Extended Authorization transaction deliberately, i.e. because the transaction is performed with the only purpose of creating a card reference, the terminal shall return a specific Response Code, RC = 'FFFD' (Transaction interrupt request) in the response to the *Submit Card Reference* command.

PIN Entry

- 2-5.7.3.6 A If PIN entry is required as the CVM, the PIN entry must be performed according to ref. 27: "TAPA, Application Architecture Specification".

Response

When the PSAM has responded to the *Initiate MSC Payment* command, the application control is returned to the MAD-Handler.

The response to the *Initiate MSC Payment 2* command will conform to the format defined in section 2-14.6.5 page 2-14-66.

The Primary Account Number (PAN) and Card Name will be returned to the MAD-Handler in the response to the *Initiate MSC Payment* command for printing purposes.

2-5.7.4 MSC Payment

Command

By issuing a *MSC Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

- 2-5.7.4.1 A The *MSC Payment* command shall conform to the format defined in section 2-14.6.7 page 2-14-71.

In case the PSAM determines that an offline transaction shall be initiated, the PSAM will provide the necessary card data to the Merchant Application Handler for performing a Stop List check.

Response

When the PSAM has responded to the *MSC Payment* command, the application control is returned to the MAD-Handler.

The response to the *MSC Payment* command will conform to the format defined in section 2-14.6.7 page 2-14-71.

2-5.7.5 Validate Data

Command

By issuing a *Validate Data 2* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

NOTE: The *Validate Data 2* command may consist of one or two segments depending of the amount of data.

- 2-5.7.5.1 A The *Validate Data 2* command shall conform to the format defined in section 2-14.6.3 page 2-14-59.

Response

Although the Application Status Words (ASW1- ASW2) indicates declined (e.g. '1221' incorrect PIN), the terminal shall continue as stated in requirement 2-5.4.5.2 page 2-5-22.

2-5.7.6 Complete Payment

Command

By issuing a *Complete Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the Data Store Handler (e.g. if an offline transaction is performed) and the Merchant Application Handler if logging of transaction data is enabled.

- 2-5.7.6.1 A The *Complete Payment* command shall conform to the format defined in section 2-14.6.8 page 2-14-73.

Response

The response to the *Complete Payment* command will conform to the format defined in section 2-14.6.8 page 2-14-73.

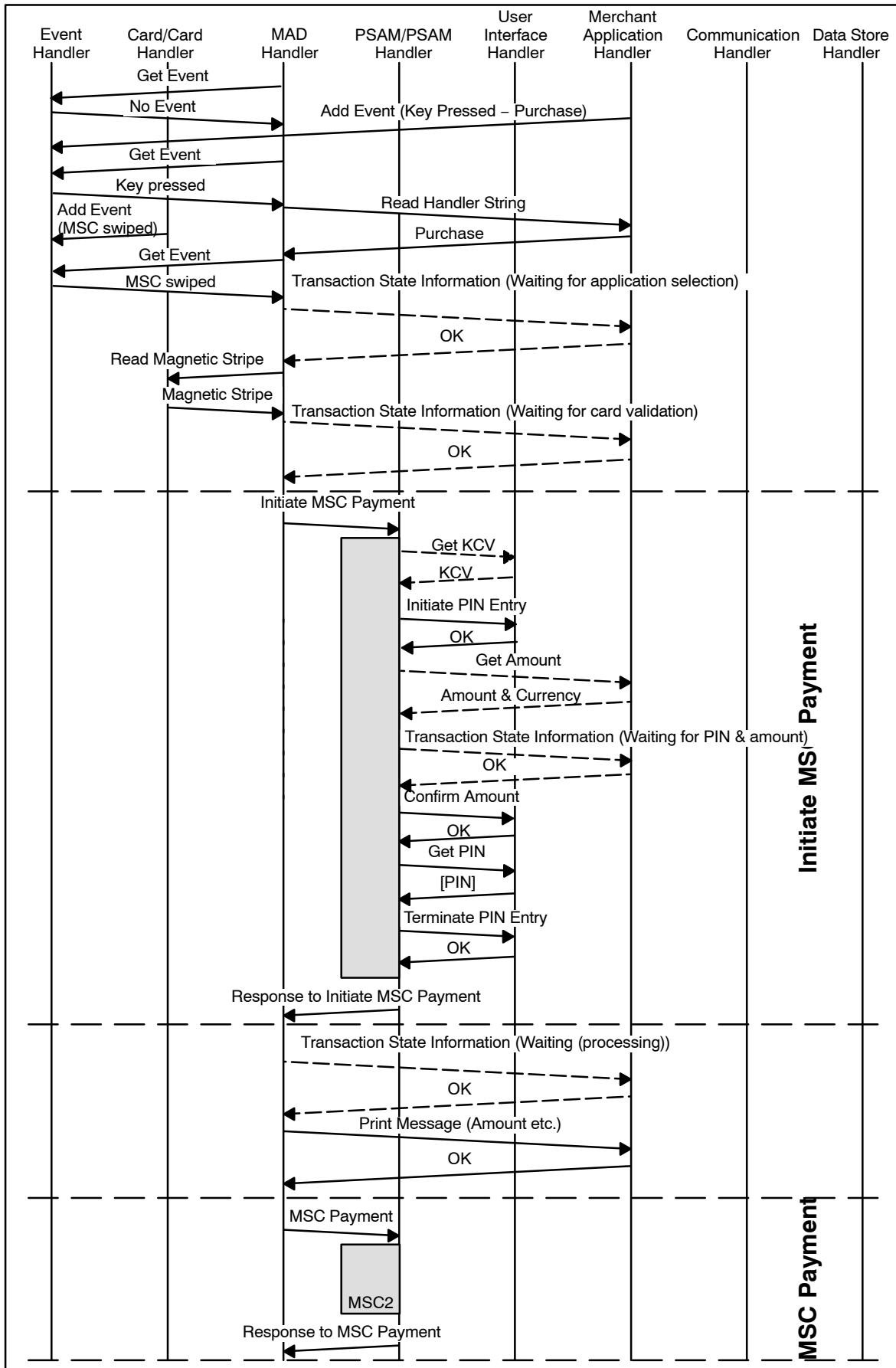


Figure 2-5.13 - MSC Transaction (Purchase - PIN)

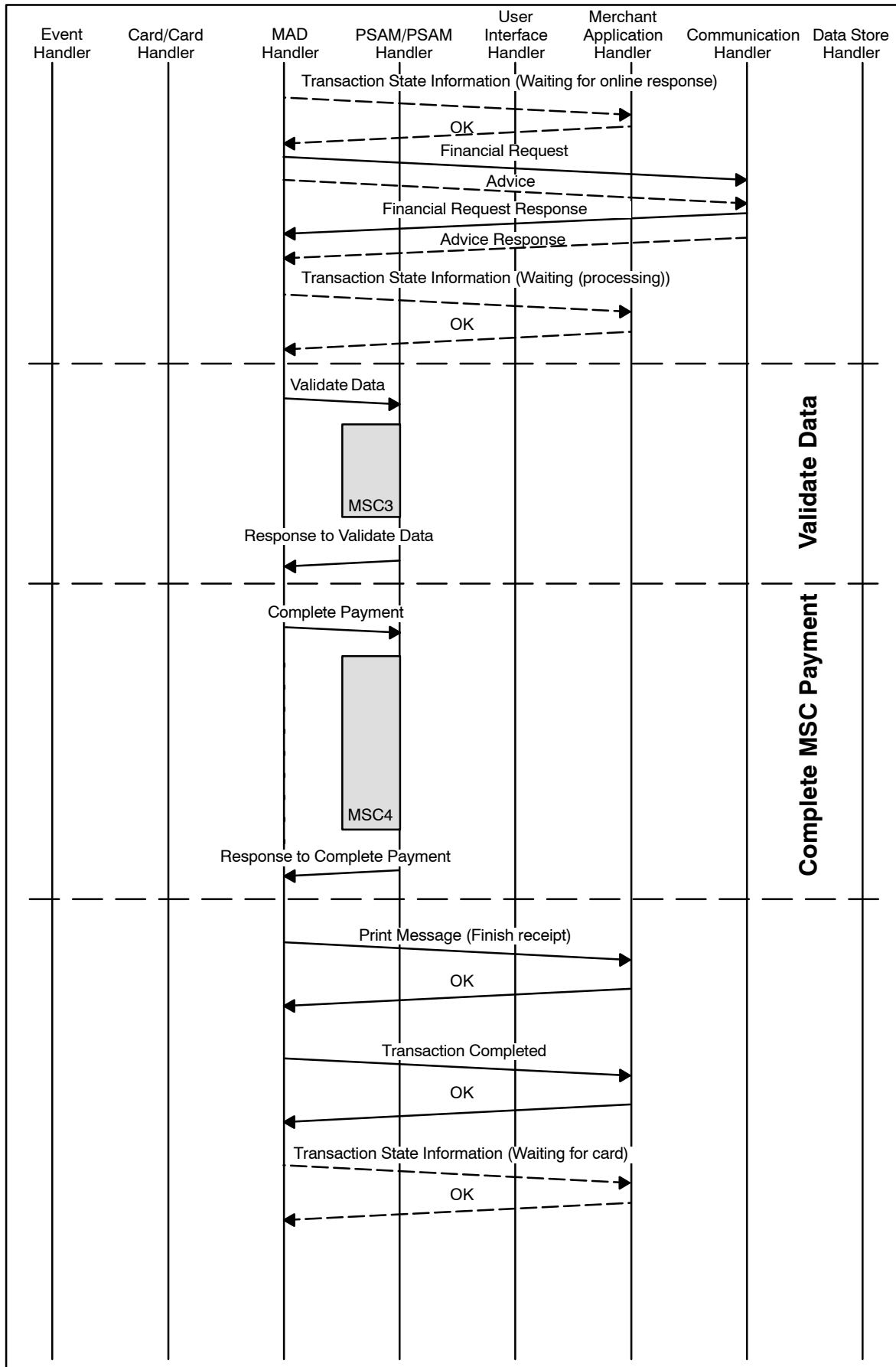


Figure 2-5.13 - MSC Transaction (Purchase - PIN) (concluded)

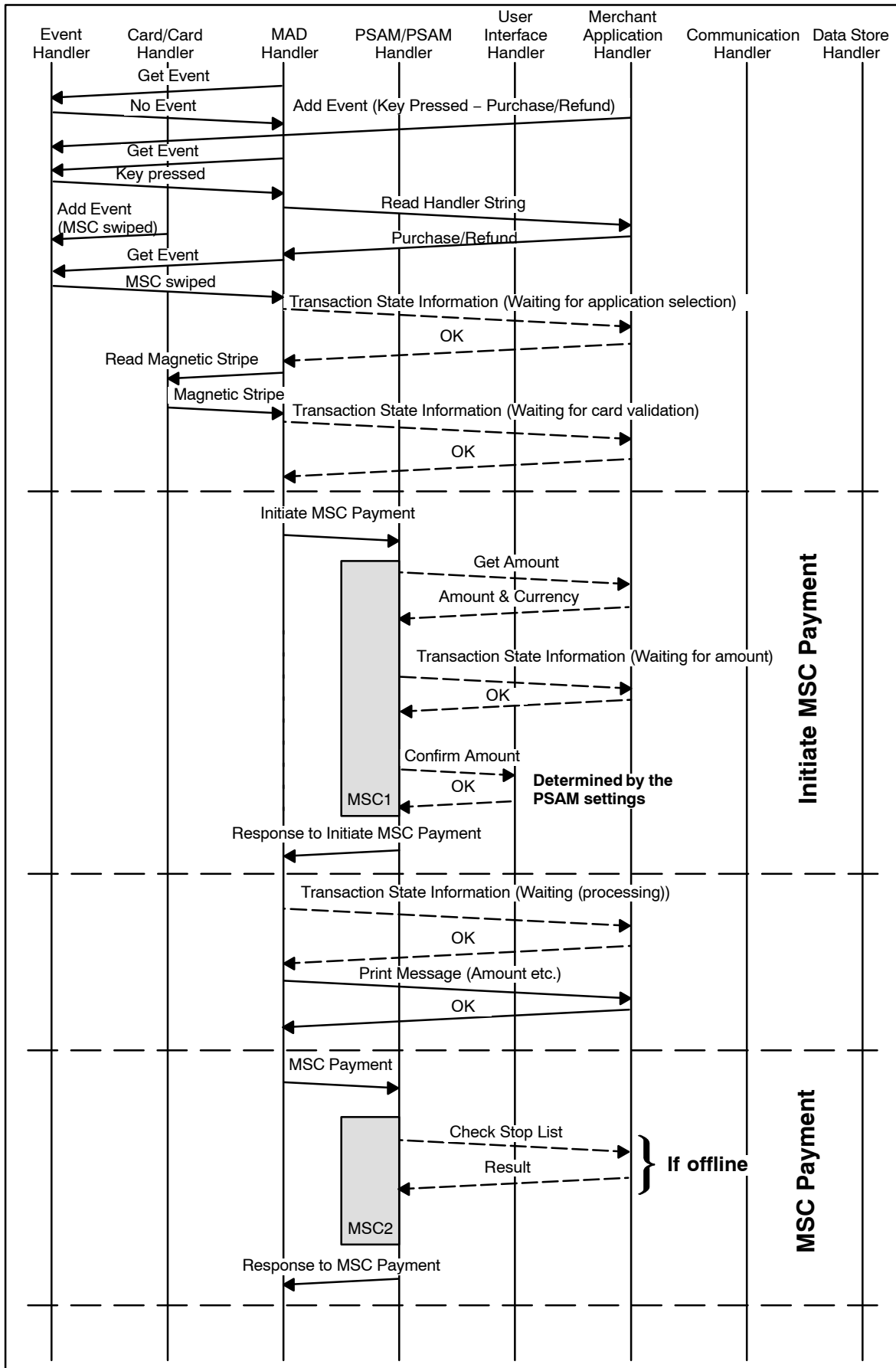


Figure 2-5.14 - MSC Transaction (Purchase/Refund - Signature)

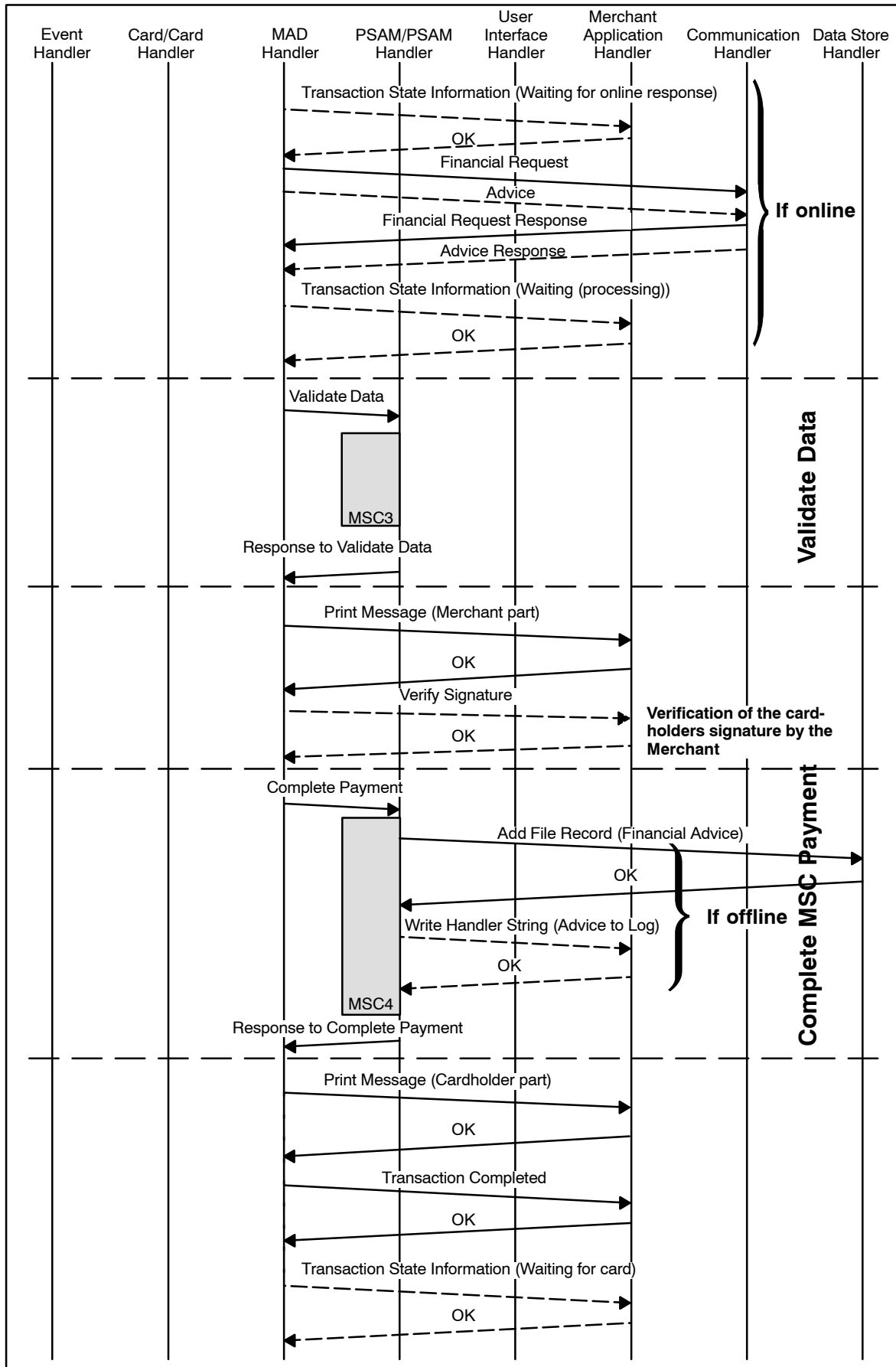


Figure 2-5.14 - MSC Transaction (Purchase/Refund - Signature) (concluded)

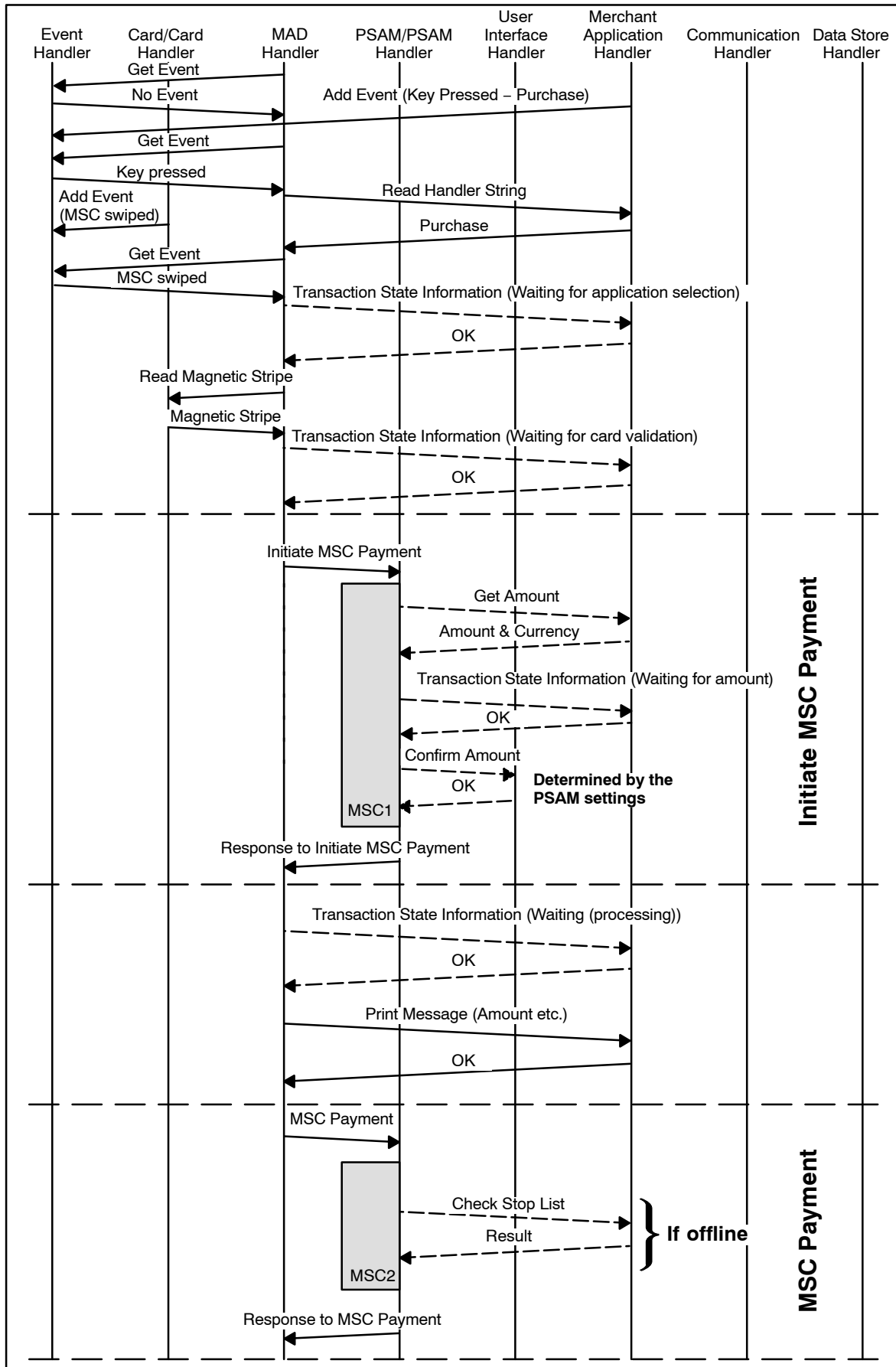


Figure 2-5.15 - MSC Transaction (Purchase - No CVM)

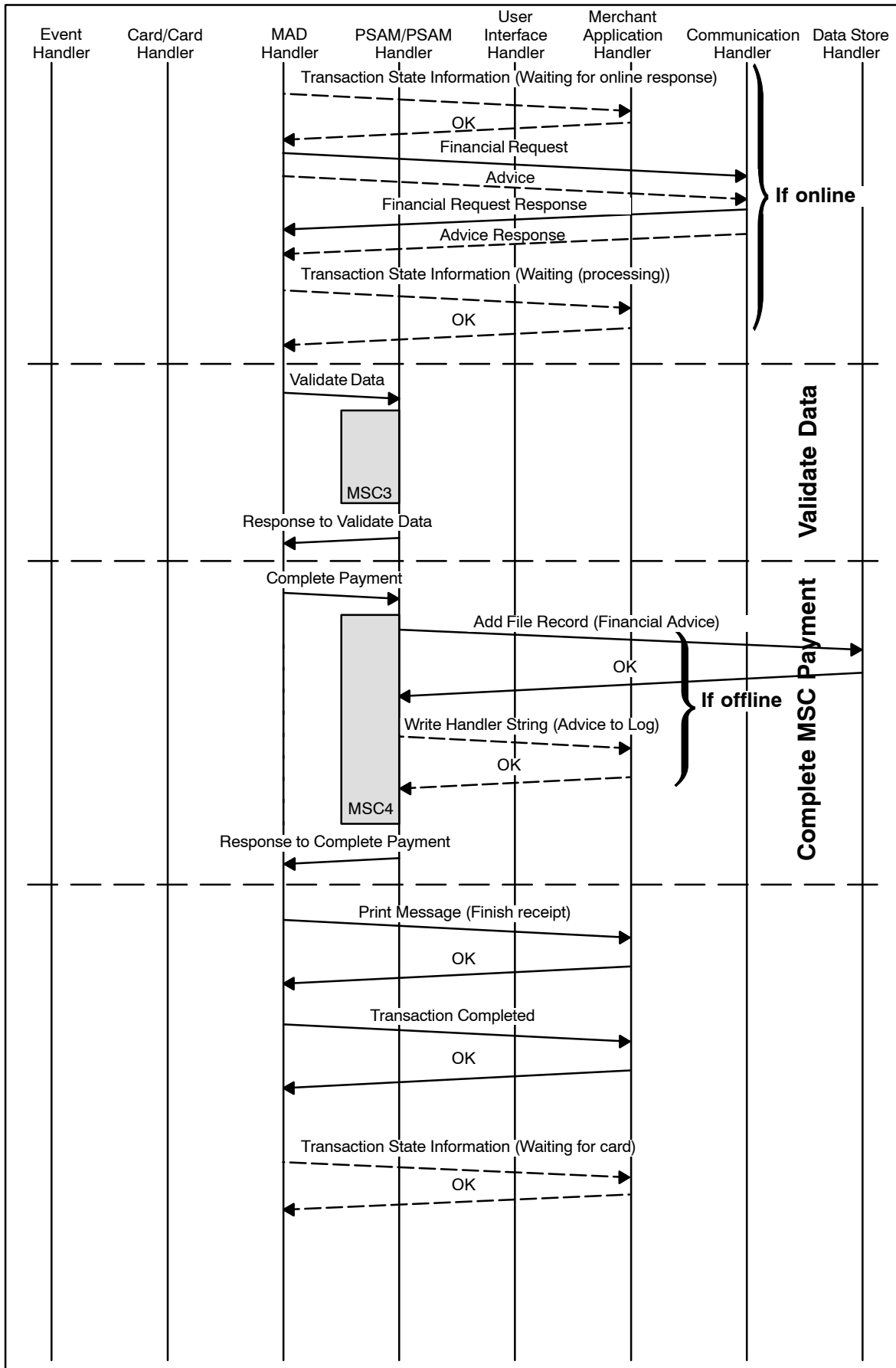


Figure 2-5.15 - MSC Transaction (Purchase - No CVM) (concluded)

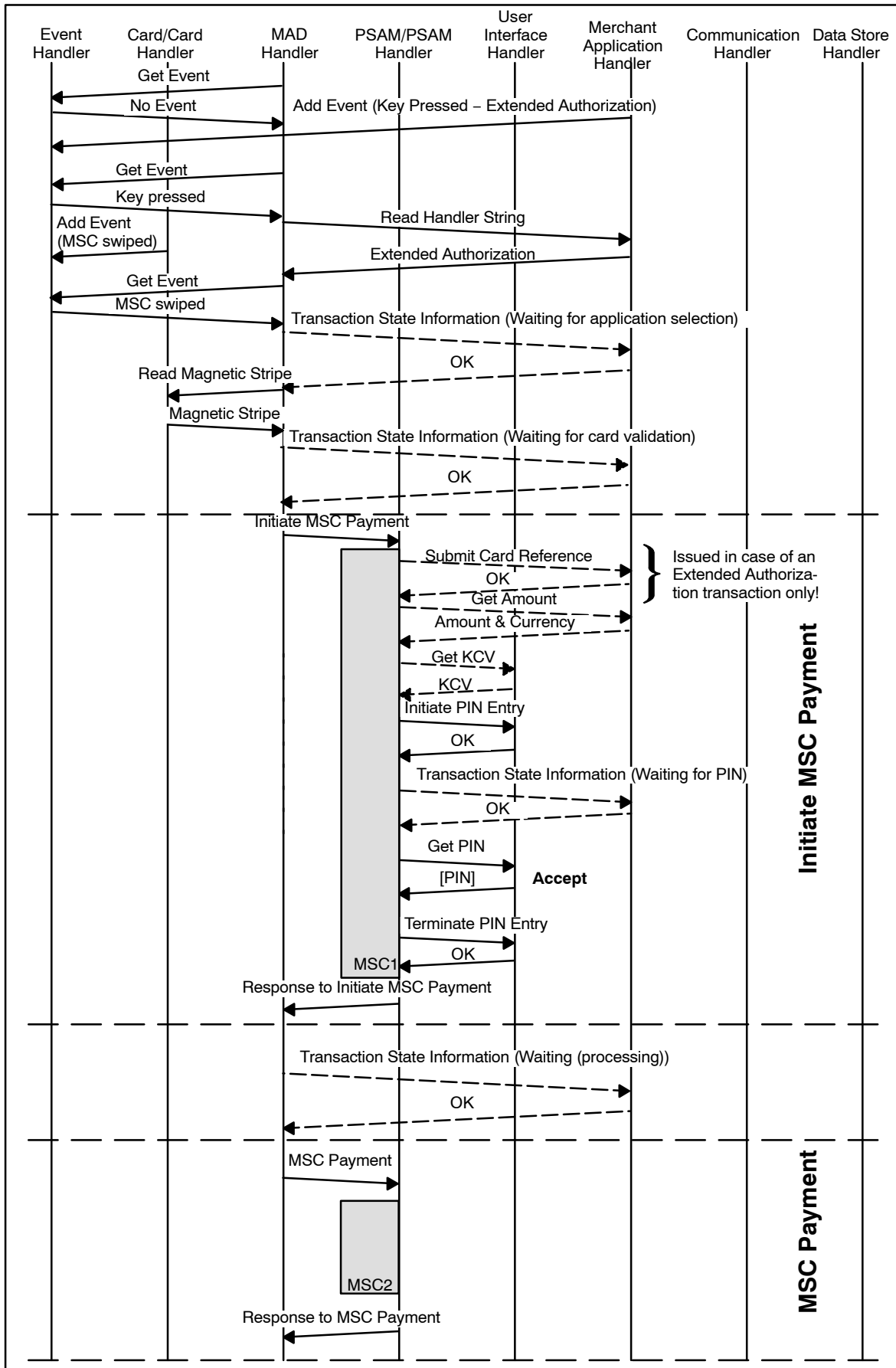


Figure 2-5.16 - MSC Transaction (Original/Extended Authorization - PIN)

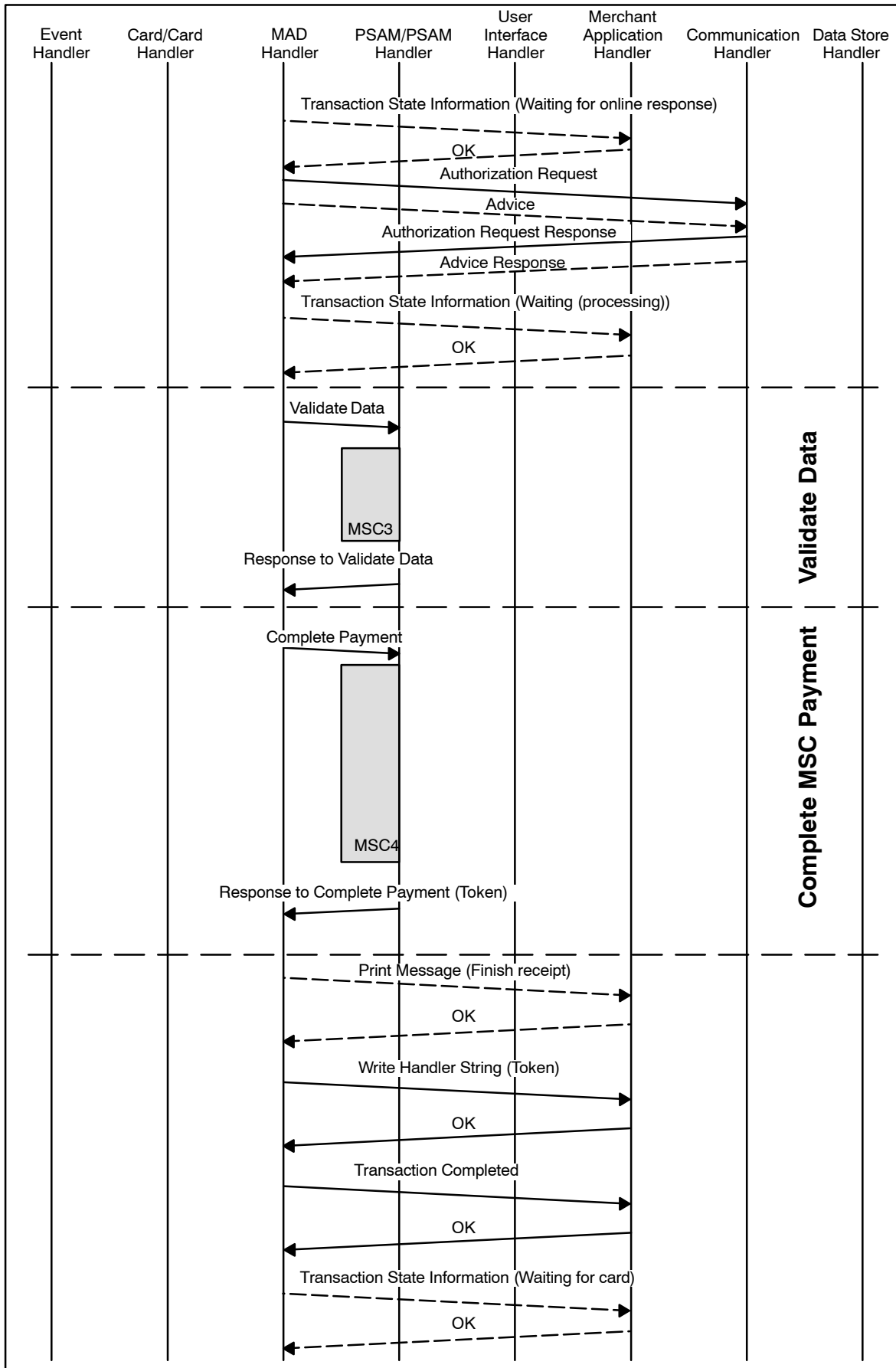


Figure 2-5.16 - MSC Transaction (Original/Extended Authorization - PIN) (concluded)

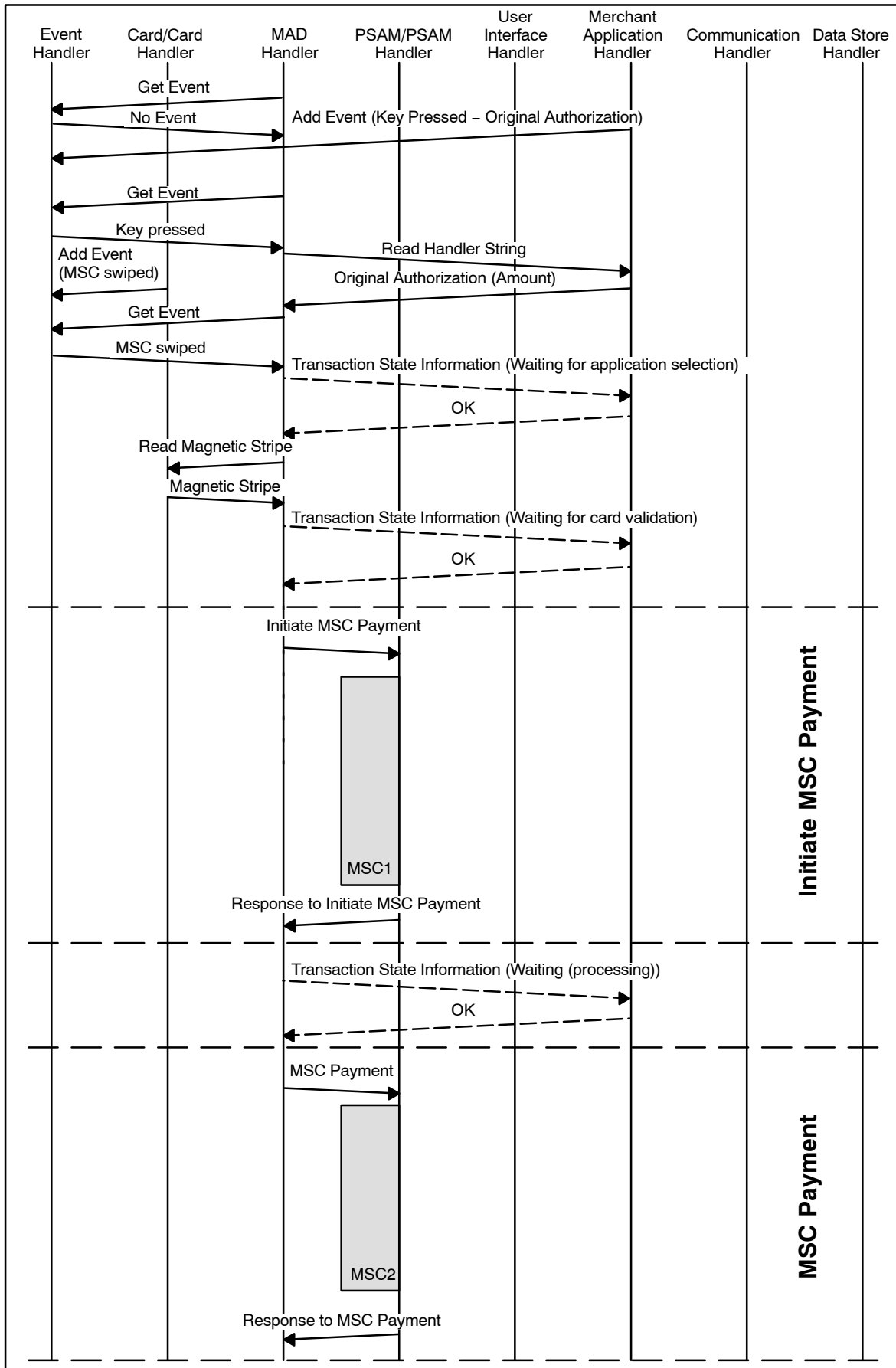


Figure 2-5.17 - MSC Transaction (Original Authorization - No CVM)

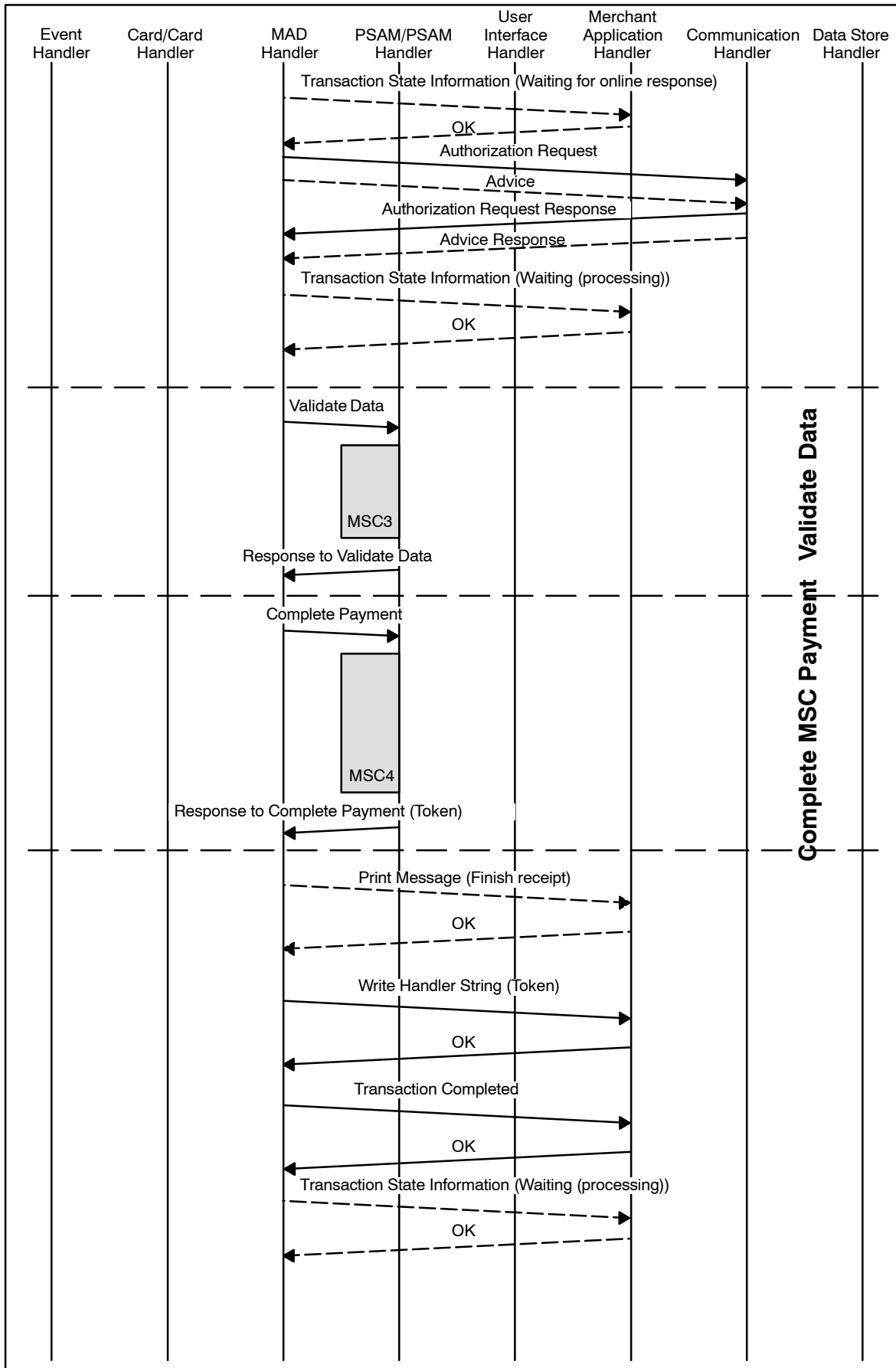


Figure 2-5.17 - MSC Transaction (Original Authorization - No CVM) (concluded)

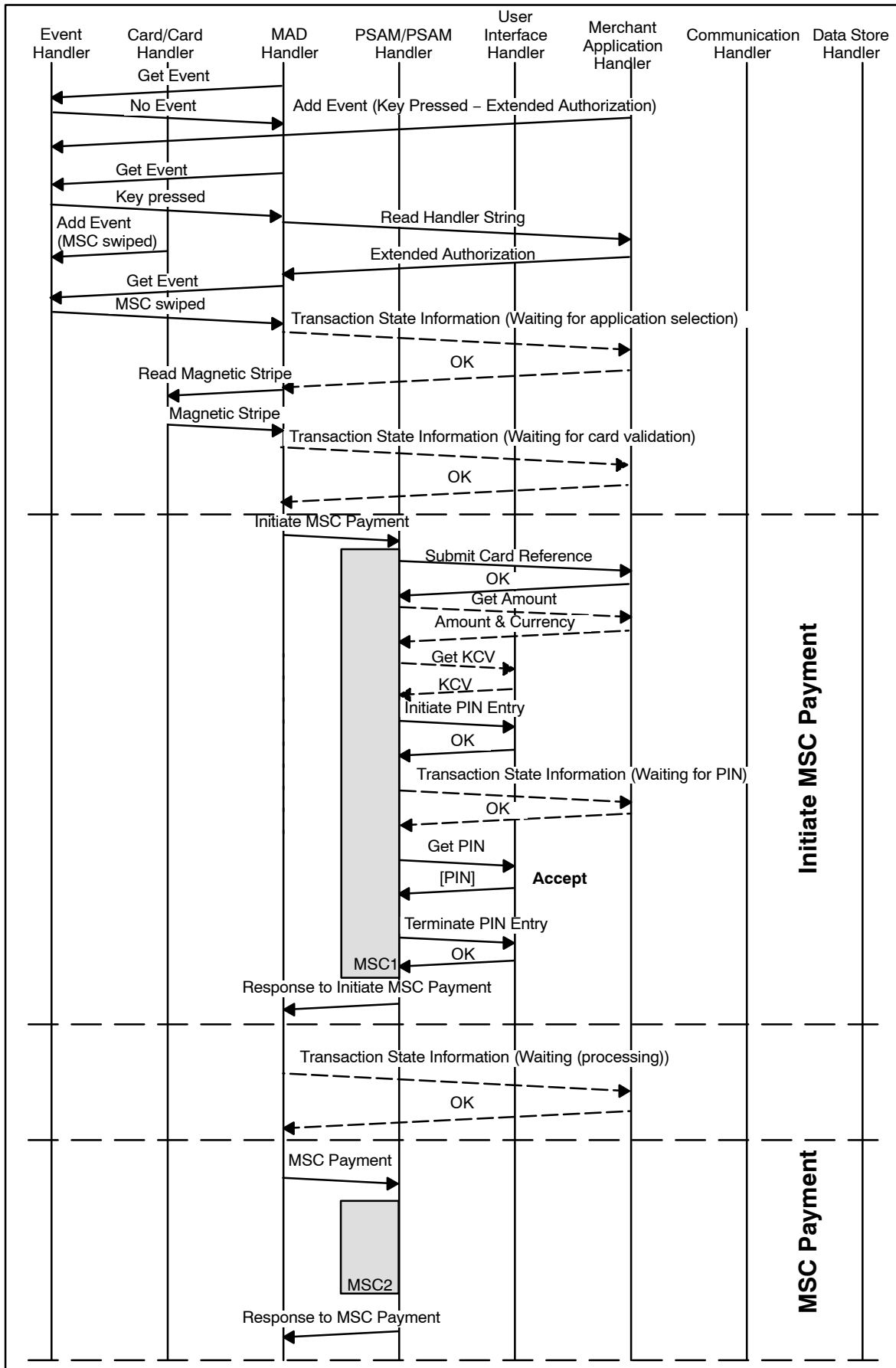


Figure 2-5.18 - MSC Transaction (Extended Authorization - PIN)

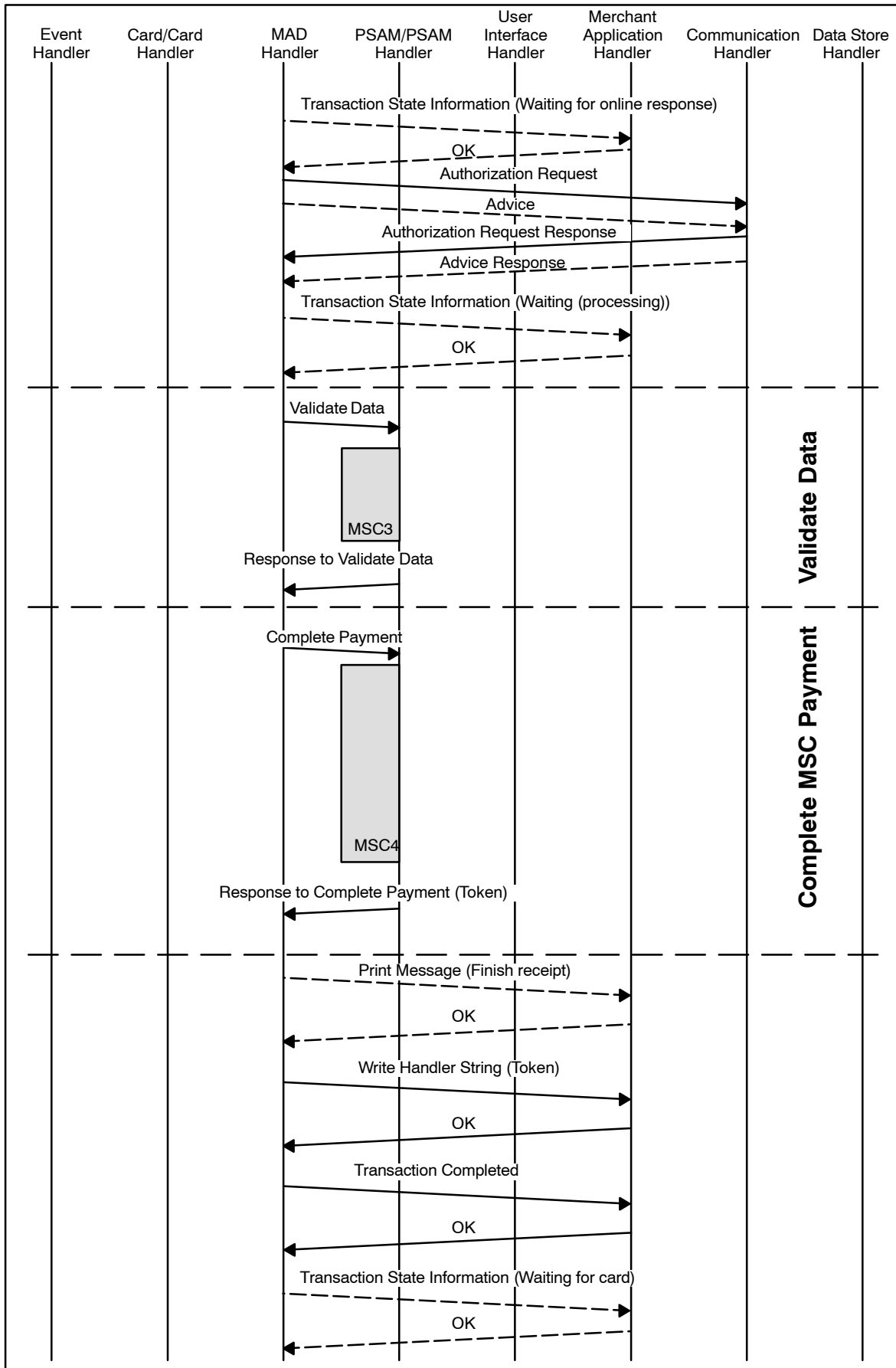


Figure 2-5.18 - MSC Transaction (Extended Authorization - PIN) (concluded)

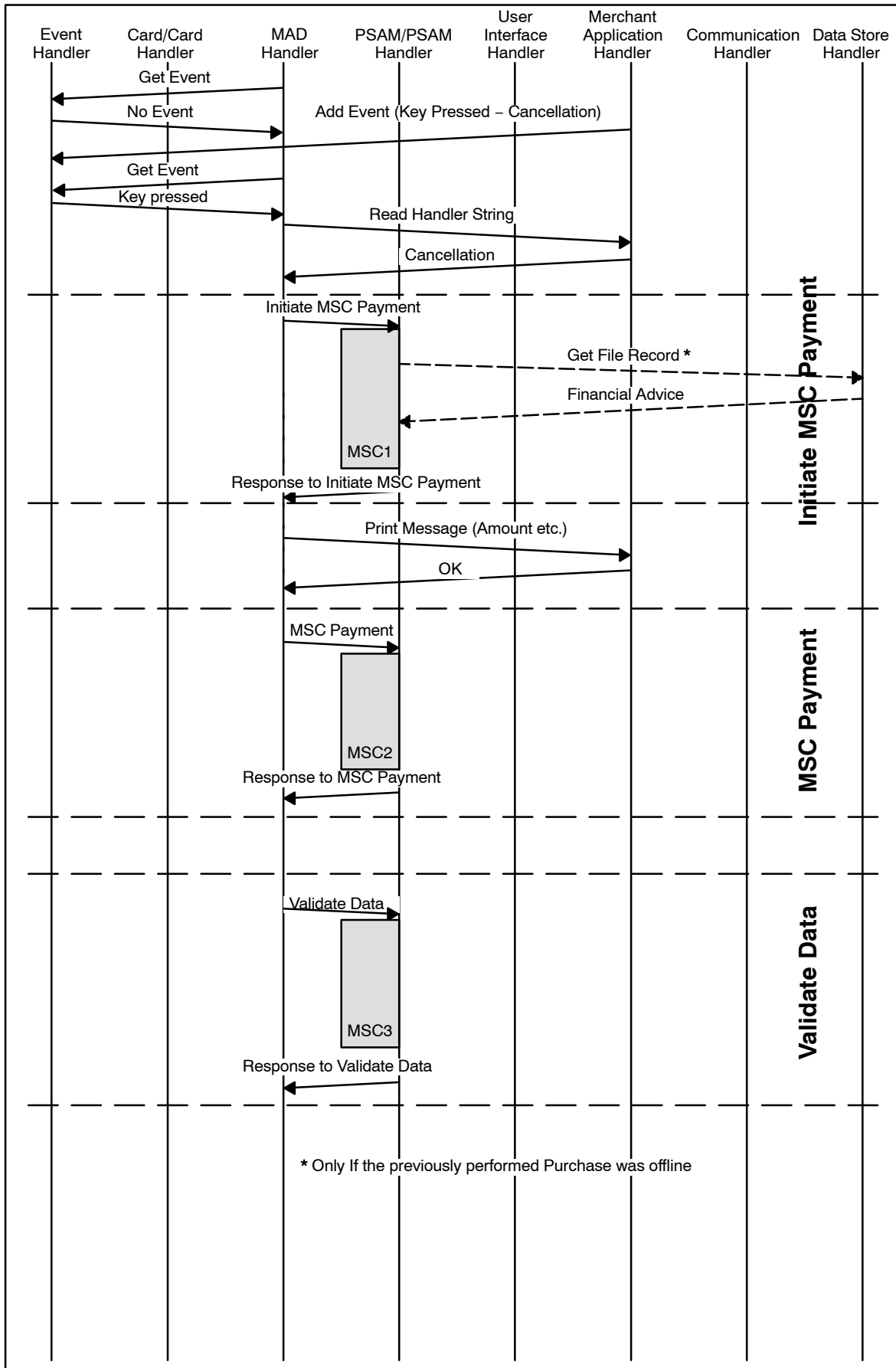


Figure 2-5.19 - MSC Transaction (Cancellation)

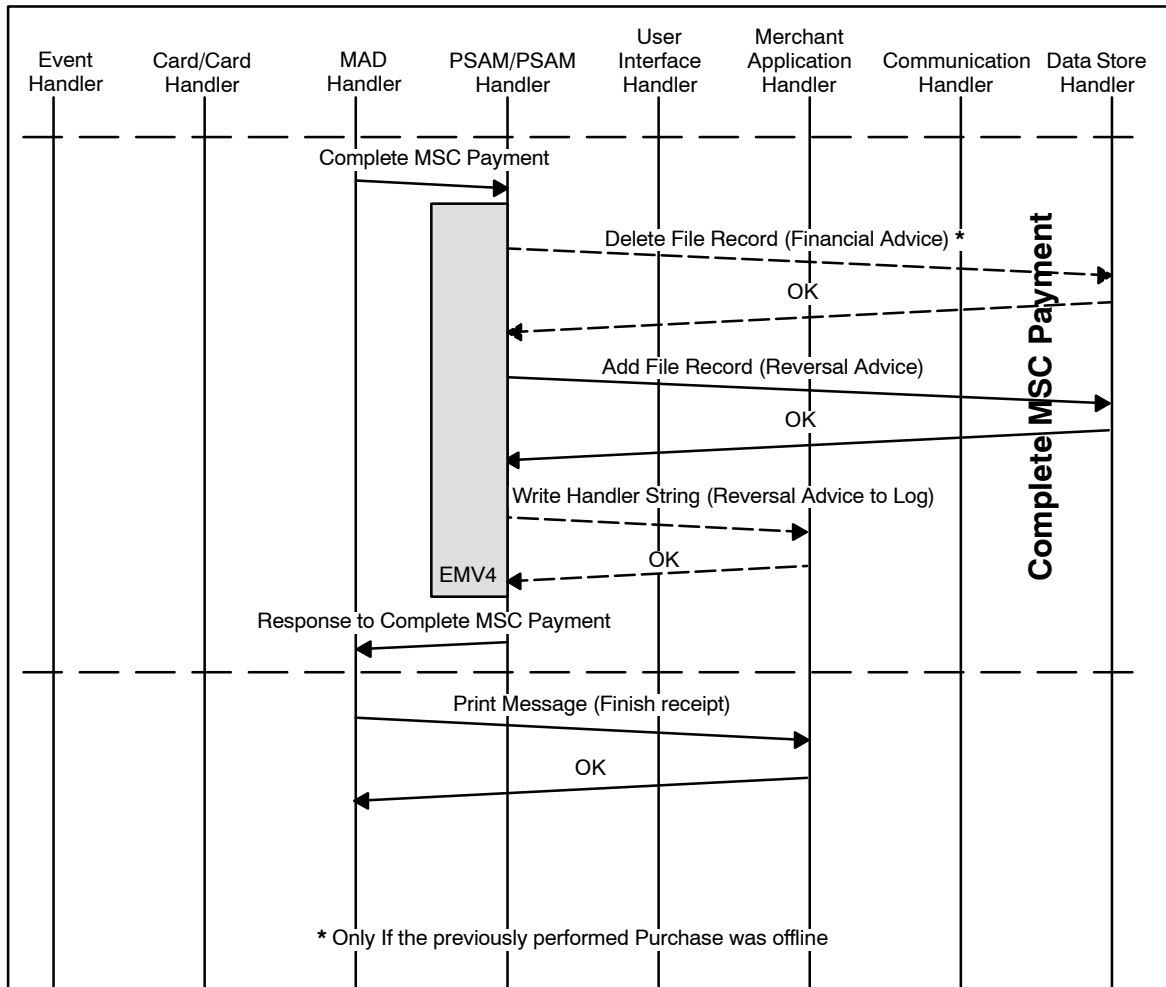


Figure 2-5.19 - MSC Transaction (Cancellation) (concluded)

2-5.8 Key Entered Card Transactions

2-5.8.1 Transaction Processing

Key entered transactions are either initiated in environments where the physical card is not present (e.g. mail order) or as a fallback (if allowed) when the track 2 of the magnetic stripe cannot be read.

Figure 2-5.20 page 2-5-65 to figure 2-5.22 page 2-5-69 provides examples of typical message flow for a successful Key Entered transactions. For a description of the handlers depicted in the figures, refer to ref. 27: "TAPA, Application Architecture Specification".

2-5.8.2 Initialization of the Key Entered Debit/Credit Payment Transaction

The way of entering the card data and initiating the Key Entered transaction is outside the scope of this specification.

- 2-5.8.2.1 A As soon as the MAD-Handler has been informed that key entered data is available, the MAD-Handler shall perform application selection based on the PAN, using the same principles as defined for magnetic stripe data in section 1-14.3.4 page 1-14-11 "MSC Application Selection".
- 2-5.8.2.2 C When the MAD-Handler application has been selected, the address information (e.g. the telephone number etc.) to use when establishing an online connection may be identified.

2-5.8.3 Initiate Key Entered Payment

Command

By issuing an *Initiate Key Entered Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the User Interface Handler and the Merchant Application Handler.

- 2-5.8.3.1 A The *Initiate Key Entered Payment* command shall conform to the format defined in section 2-14.6.9 page 2-14-74.
- 2-5.8.3.2 A The data element "Card Data Source" shall be set to '02' indicating Key Entered.

Entering the Amount

For the Purchase/Refund/Original Authorization transaction, the amount may be present before the *Initiate Key Entered Payment* command is issued. If the amount is not available in the *Initiate Key Entered Payment* command, the PSAM will obtain the amount from the Merchant Application at the appropriate time.

Response

When the PSAM has responded to the *Initiate Key Entered Payment* command, the application control is returned to the MAD-Handler.

The response to the *Initiate Key Entered Payment* command will conform to the format defined in section 2-14.6.9 page 2-14-74.

The Primary Account Number (PAN) and Card Name will be returned to the MAD-Handler in the response to the *Initiate Key Entered Payment* command for printing purposes.

2-5.8.4 Key Entered Payment

Command

By issuing an *Key Entered Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

- 2-5.8.4.1 A The *Key Entered Payment* command shall conform to the format defined in section 2-14.6.11 page 2-14-79.

In case the PSAM/terminal determines that an offline transaction shall be initiated, the PSAM will provide the necessary card data to the Merchant Application Handler for performing a Stop List check.

Response

When the PSAM has responded to the *Key Entered Payment* command, the application control is returned to the MAD-Handler.

The response to the *Key Entered Payment* command will conform to the format defined in section 2-14.6.11 page 2-14-79.

2-5.8.5 Validate Data

Command

By issuing a *Validate Data 2* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

NOTE: The *Validate Data 2* command may consist of one or two segments depending of the amount of data.

- 2-5.8.5.1 A The *Validate Data 2* command shall conform to the format defined in section 2-14.6.3 page 2-14-59.

Response

See section 2-5.4.5 page 2-5-22

2-5.8.6 Complete Key Entered Payment

Command

By issuing a *Complete Key Entered Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the Data Store Handler (e.g. if an offline transaction is performed) and the Merchant Application Handler if logging of transaction data is enabled.

- 2-5.8.6.1 A The *Complete Key Entered Payment* command shall conform to the format defined in section 2-14.6.12 page 2-14-81.

Response

The response to the *Complete Key Entered Payment* command will conform to the format defined in section 2-14.6.12 page 2-14-81.

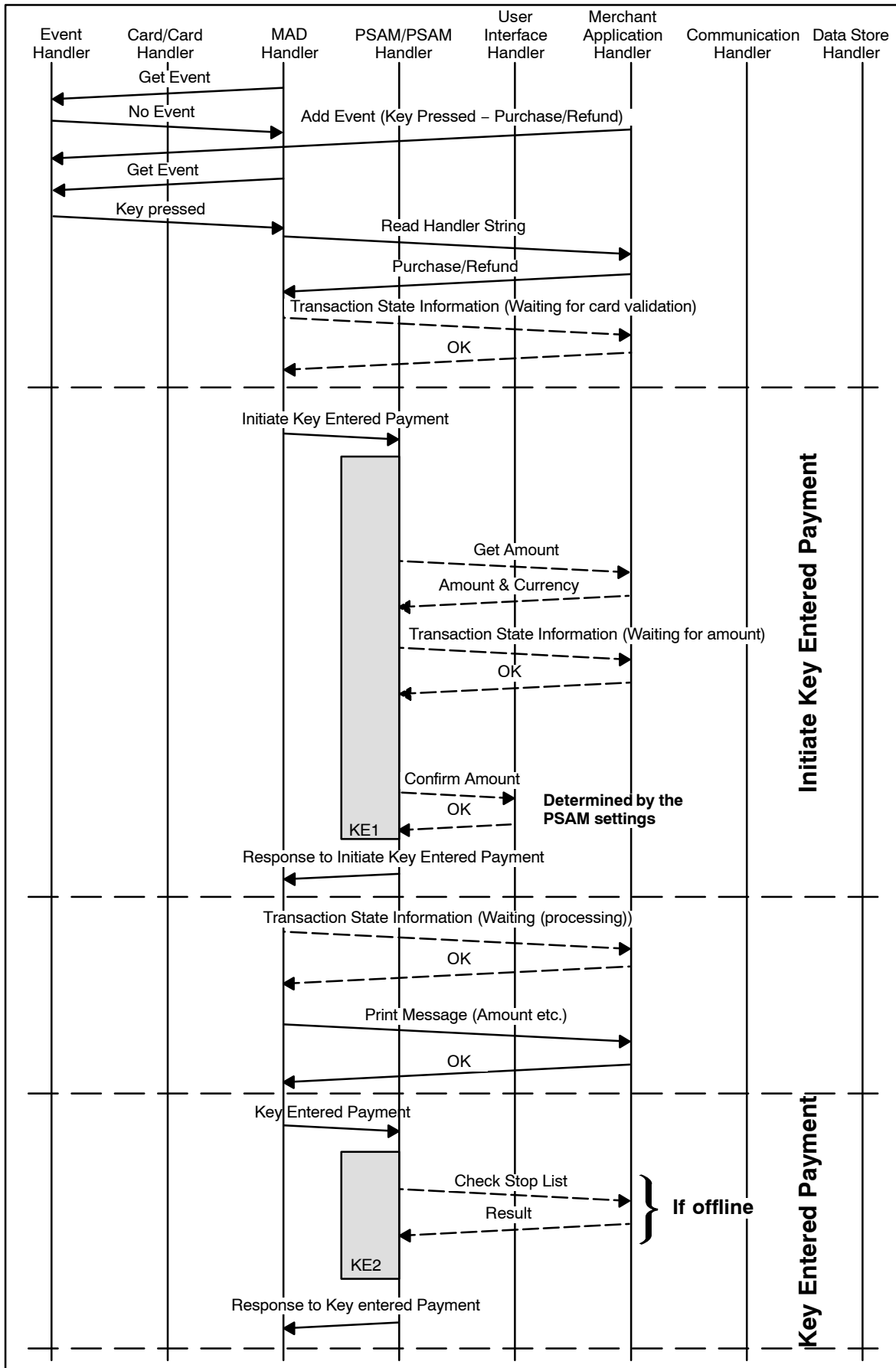


Figure 2-5.20 - Key Entered Transaction (Purchase/Refund - Signature)

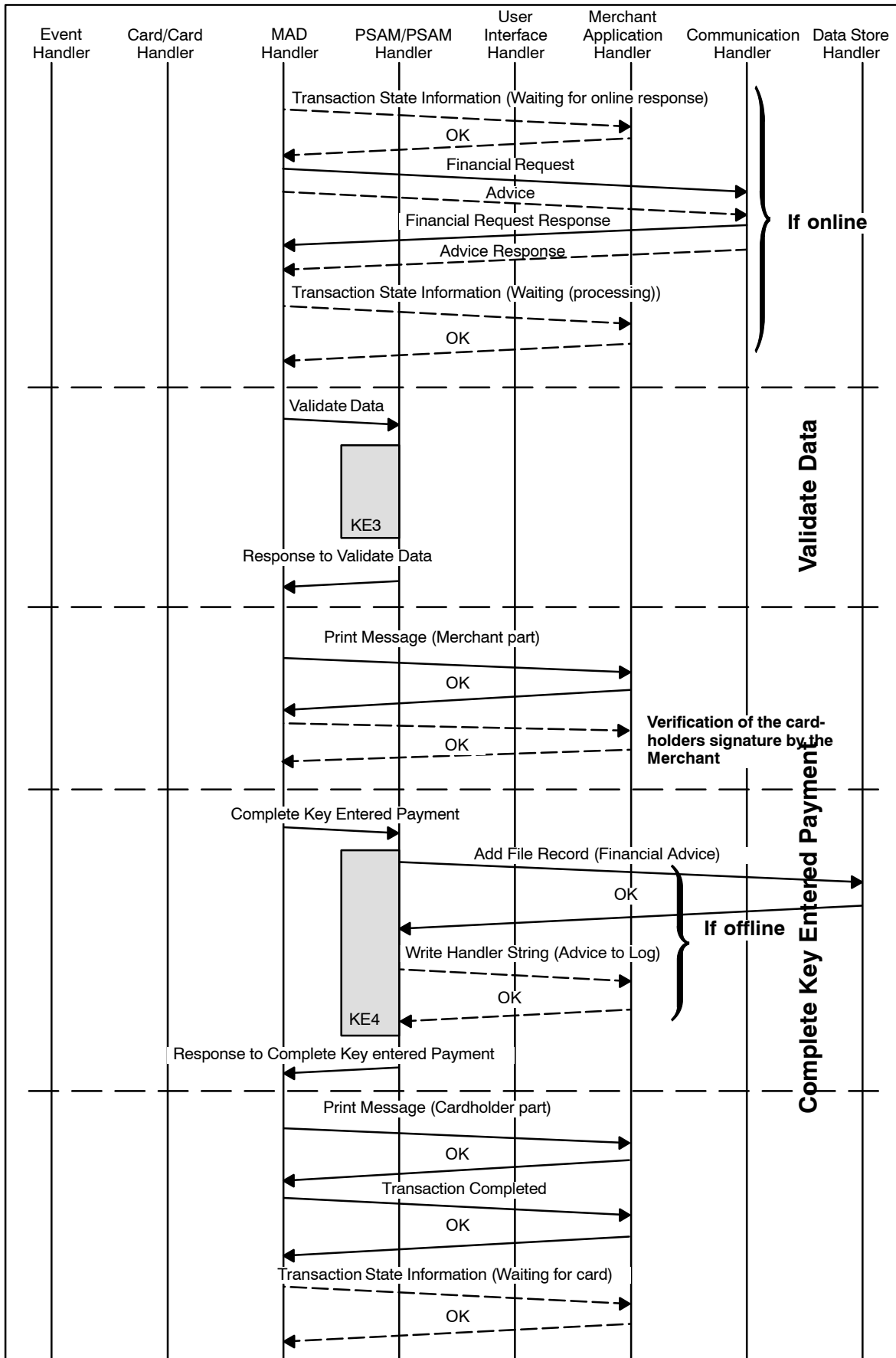


Figure 2-5.20 - Key Entered Transaction (Purchase/Refund - Signature) (concluded)

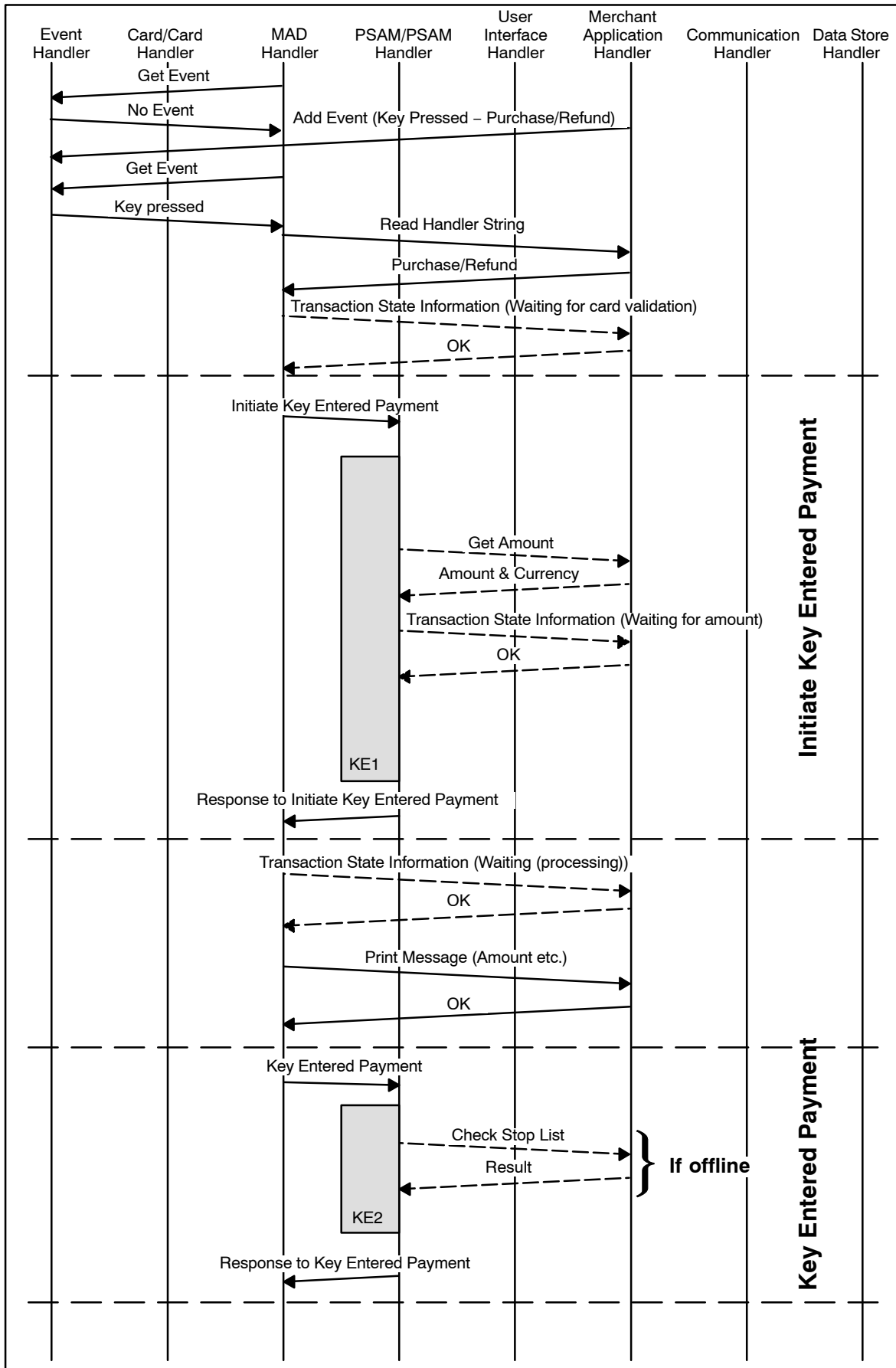


Figure 2-5.21 - Key Entered Transaction (Purchase/Refund - No CVM)

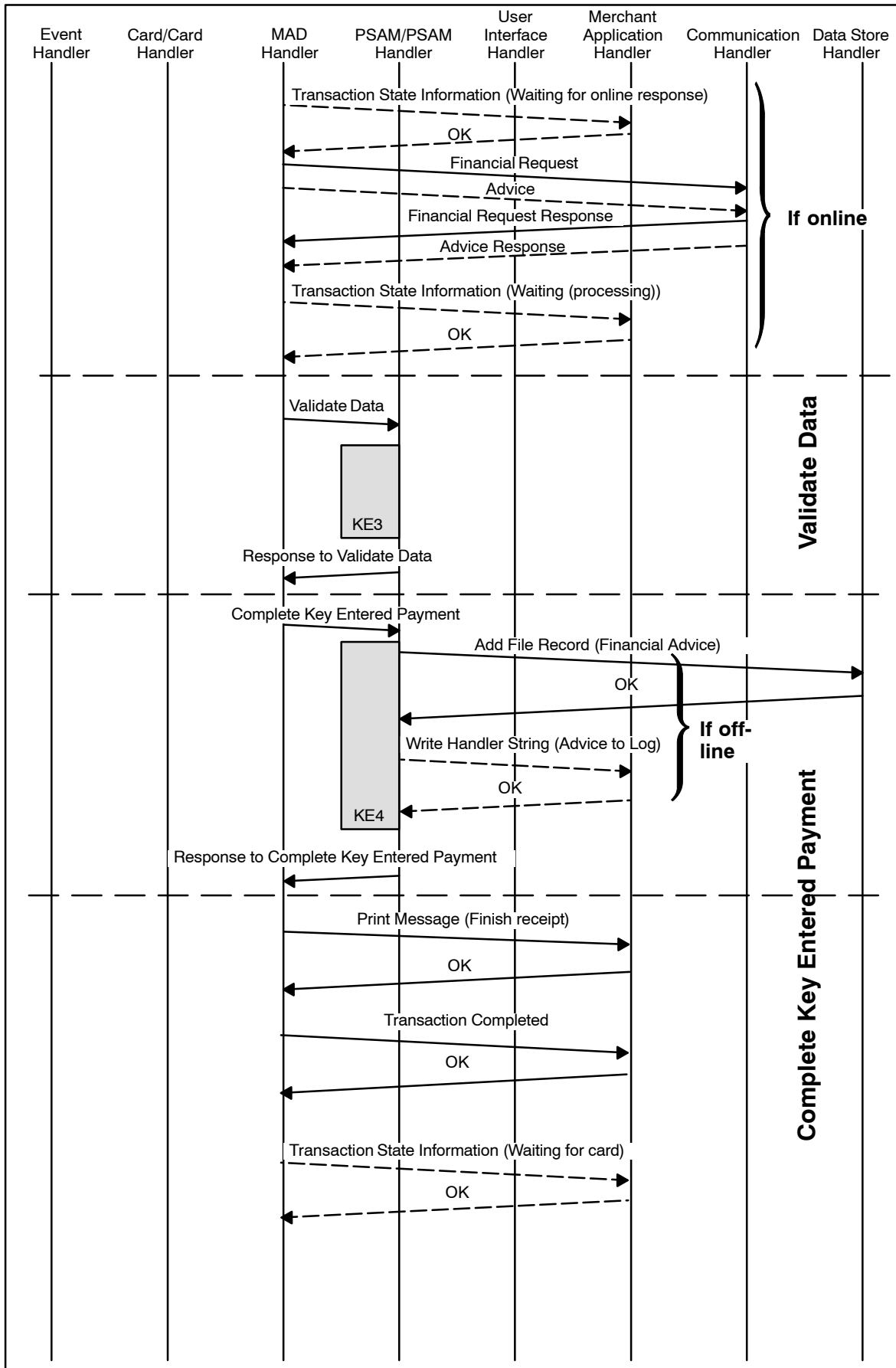


Figure 2-5.21 - Key Entered Transaction (Purchase - No CVM) (concluded)

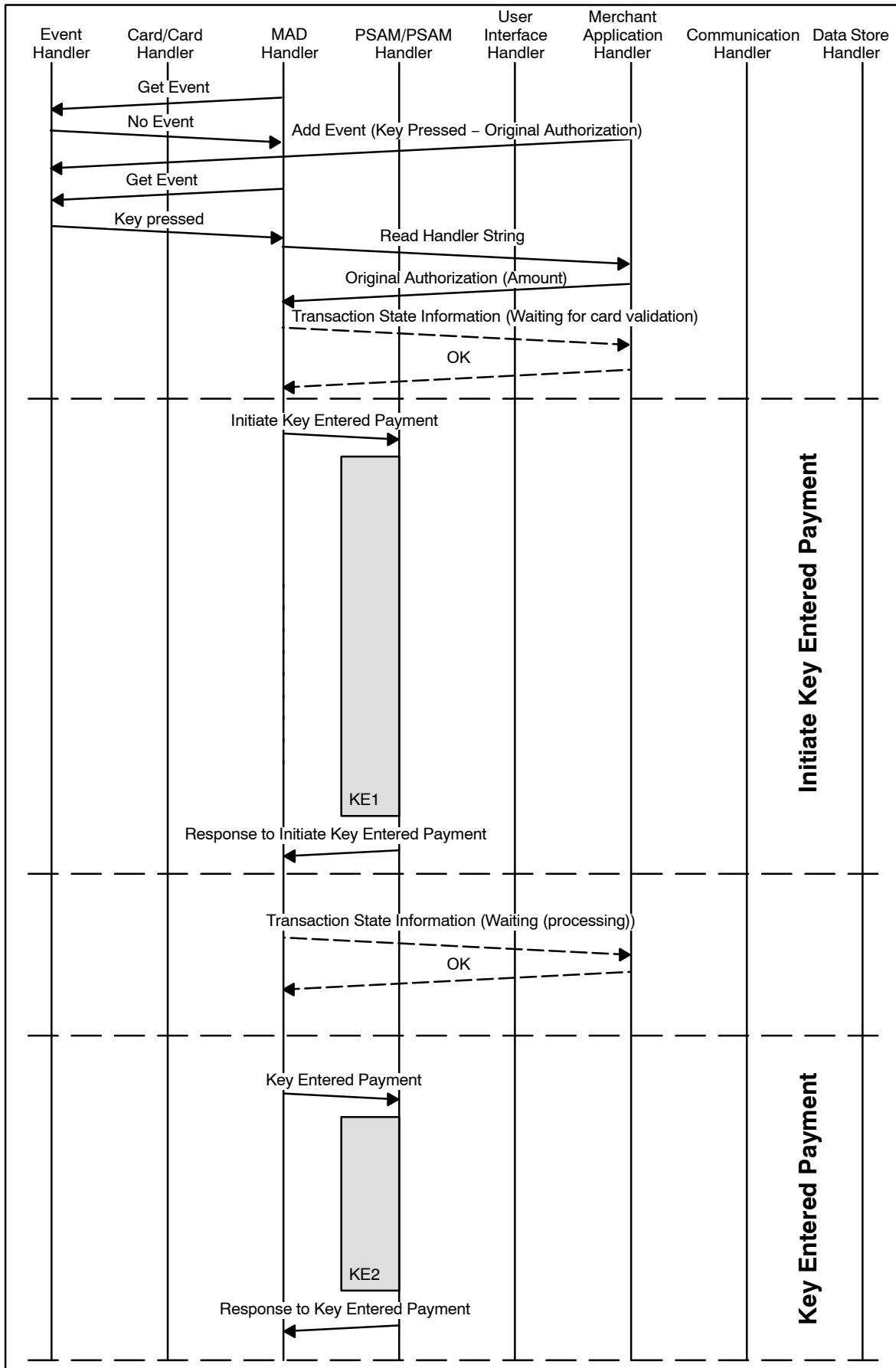


Figure 2-5.22 - Key Entered Transaction (Original Authorization - No CVM)

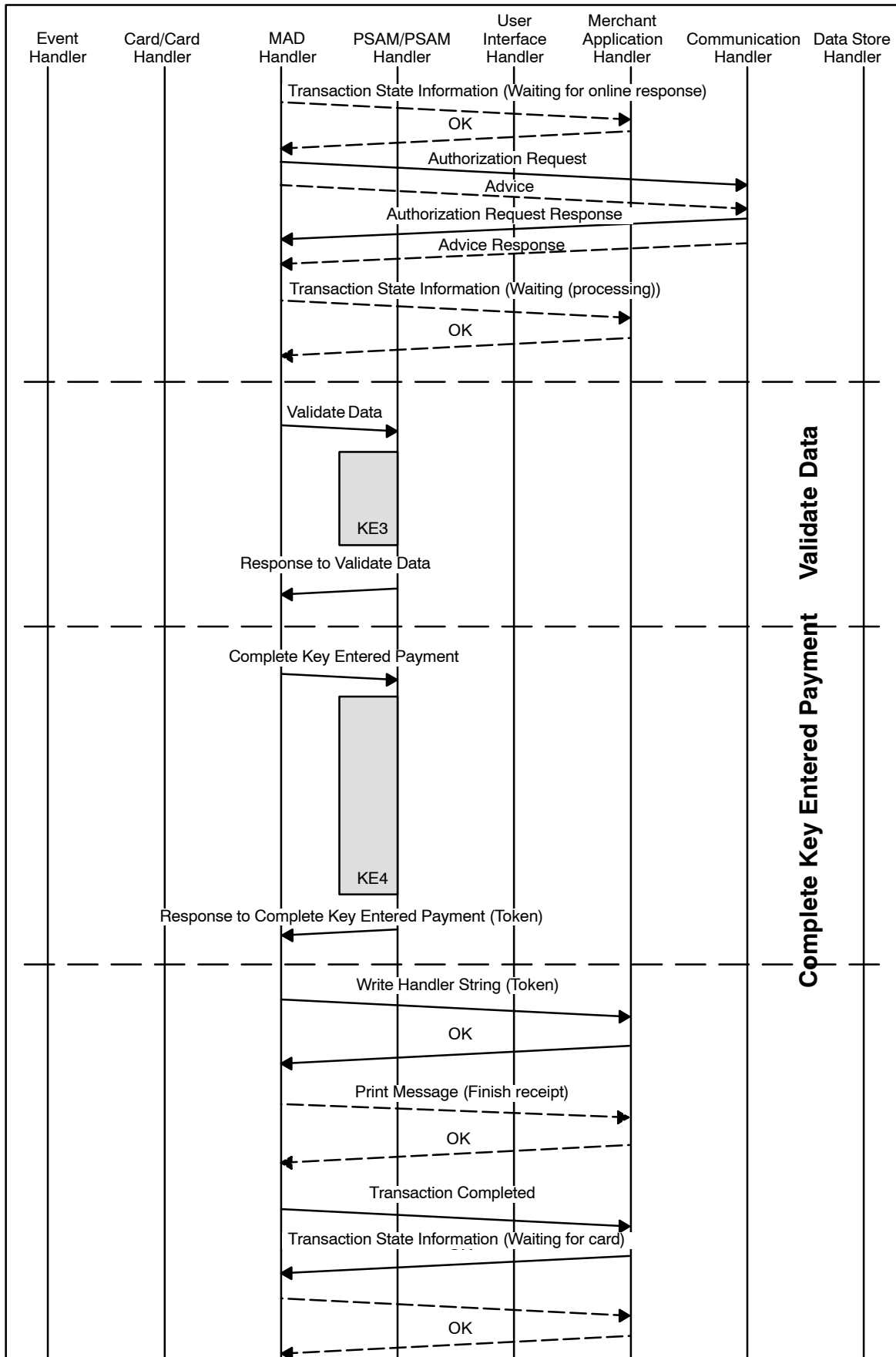


Figure 2-5.22 - Key Entered Transaction (Original Authorization - No CVM) (concluded)

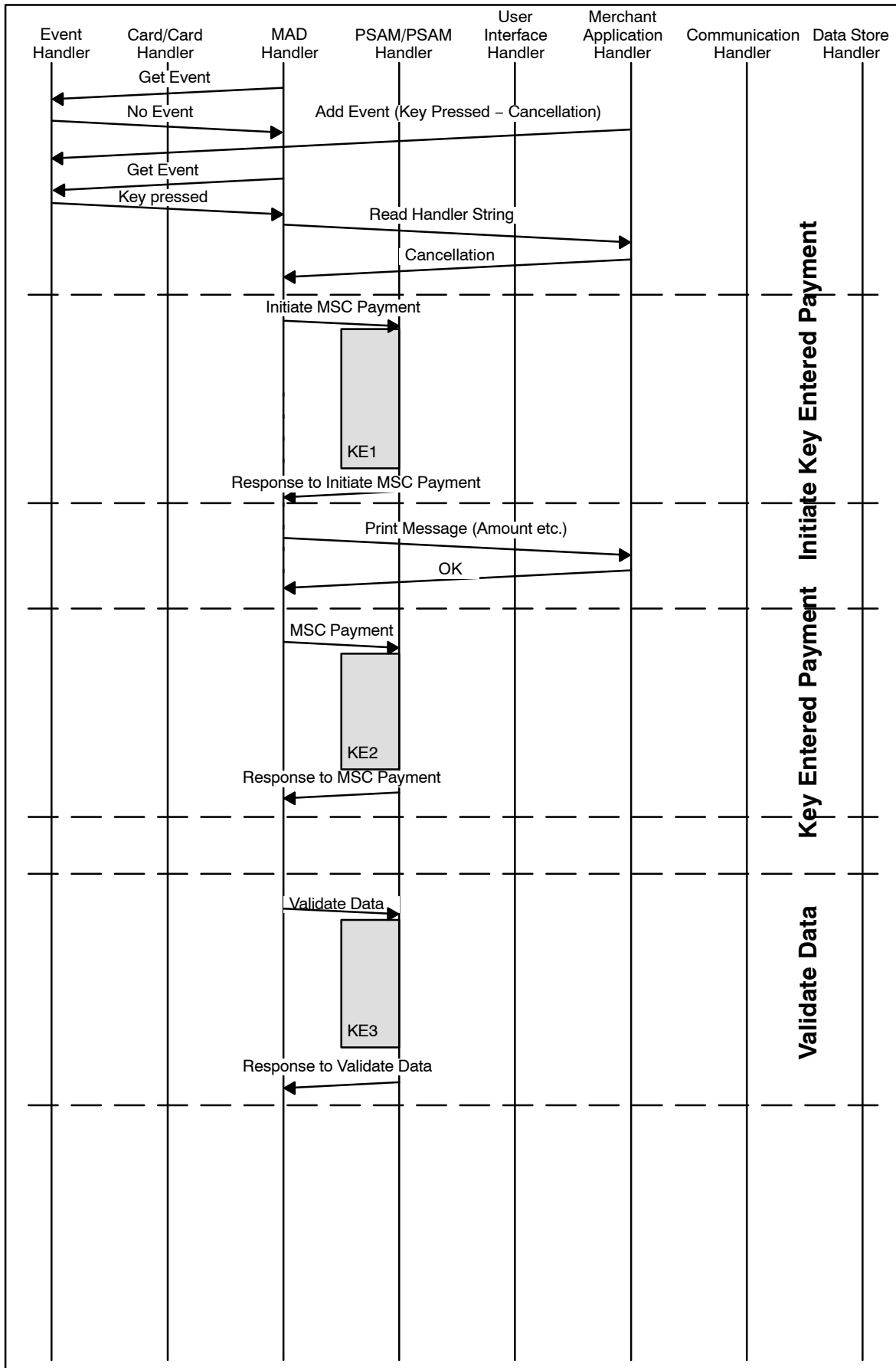


Figure 2-5.23 - Key Entered Transaction (Cancellation)

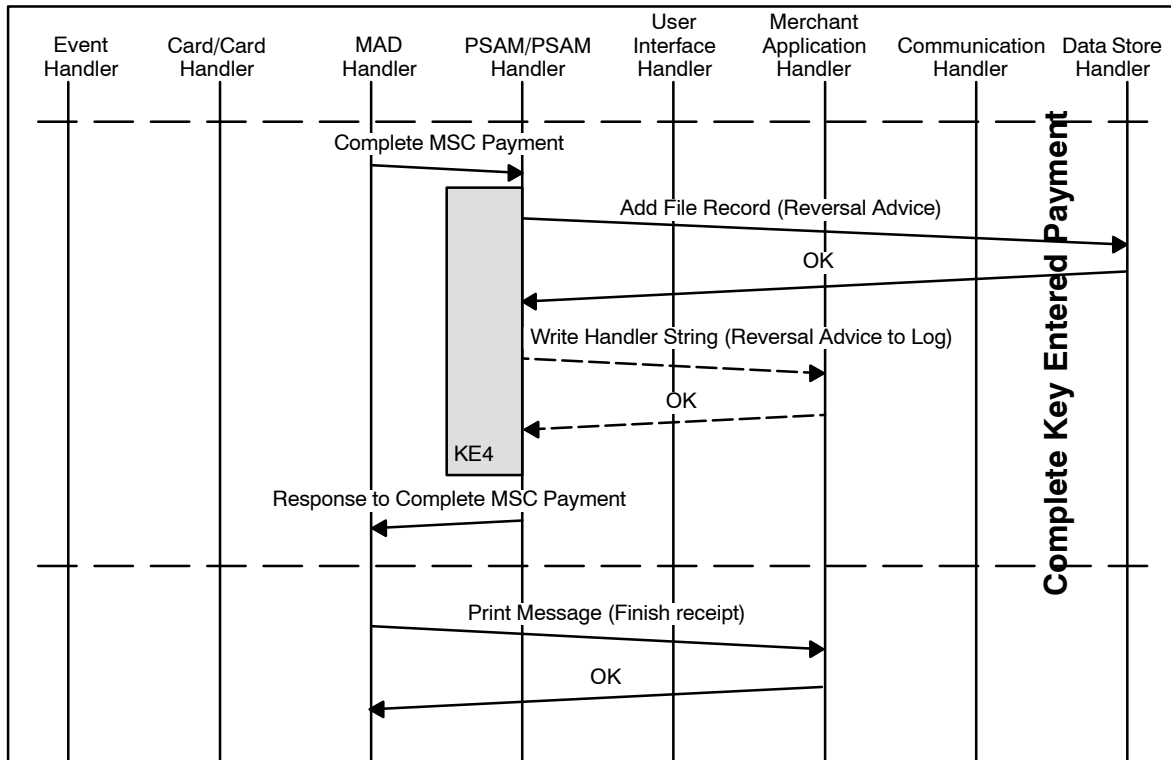


Figure 2-5.23 - Key Entered Transaction (Cancellation) (concluded)

2-5.9 Token based Transactions

2-5.9.1 Transaction Processing

The Merchant Application initiates the transaction by using the appropriate Business Call.

Token based transactions includes the following transactions:

- Supplementary Authorization
- Capture
- Reversal (Authorization)

NOTE: Although an Original/Extended Authorization results in Token as output, this transaction is not part of the Token based transactions. See section 2-5.3 page 2-5-16, 2-5.4 page 2-5-20, 2-5.5 page 2-5-23 and 2-5.7 page 2-5-45 for further details.

Figures 2-5.24 page 2-5-76 to 2-5.27 page 2-5-82 provides examples of typical message flows for successful Token Based transactions. For a description of the handlers depicted in the figures, refer to ref. 27: "TAPA, Application Architecture Specification".

2-5.9.2 Initialization of the Token Based Debit/Credit Payment Transaction

The retrieval of the Token from the Merchant Application is business dependent. Example, for payment of a rental car, the Token may be linked to the reference number of the rental contract.

The way of retrieving the correct Token is outside the scope of this specification.

- 2-5.9.2.1 A The two data elements from the Info field of the Token (Token Format and $LEN_{AID} + AID/Prefix$) shall be transferred to the MAD-Handler.

NOTE: The data elements should e.g. be transferred by the *Read Handler String* command.

- 2-5.9.2.2 A As soon as the MAD-Handler has been informed that a Token is available, the MAD-Handler shall select the "right" PSAM based on the AID/Prefix from the Info field of the Token.

NOTE: Based on the data element Token Format the MAD-Handler will be able to identify the original card data source. Selection of transaction processing will then be based on either the Application Identifier or the PAN-prefix, using the principles defined in respectively section 1-14.3.5 page 1-14-12 , ICC Application Selection," and section 1-14.3.4 page 1-14-11, MSC Application Selection.

2-5.9.3 Initiate Token Based Payment

Command

By issuing an *Initiate Token Based Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the User Interface Handler and the Merchant Application Handler.

- 2-5.9.3.1 A The *Initiate Token Based Payment 2* command shall conform to the format defined in section 2-14.6.13 page 2-14-82.

NOTE: The Amount in the *Initiate Token Based Payment* is the final amount, i.e. the amount that will be transferred to the Merchant's account.

- 2-5.9.3.2 A The data element "Card Data Source" shall be set to '03' indicating Token Based.

- 2-5.9.3.3 A The Merchant Initiative ("MI") shall be set to '00' indicating that the merchant does not force either the transaction online/offline or force a specific CVM.

Entering the Amount

- 2-5.9.3.4 A For all Token Based transactions, the amount shall be present before the *Initiate Token Based Payment 2* command is issued.

- 2-5.9.3.5 A As Cashback is not allowed, the field Amount, Other shall either be set to zero or omitted in the *Initiate Token Based Payment 2* command.

Account Type

- 2-5.9.3.6 A For terminals where both terminal and PSAM support Service Pack No. 2, the Account Type shall be inserted as the final data element. See section 2-15.2.1 on page 2-15-2 for further details concerning Account Type.

Response

When the PSAM has responded to the *Initiate Token Based Payment* command, the application control is returned over to the MAD-Handler.

The response to the *Initiate Token Based Payment* command will conform to the format defined in section 2-14.6.13 page 2-14-82.

The Merchant Number ("ME_{NUMBER}"), which is part of the Token, will be returned. This number might be used to check if a Token created at the merchant related to the ME_{NUMBER} is accepted/valid in the present store.

The Primary Account Number (PAN) and Card Name will be returned to the MAD-Handler in the response to the *Initiate Token Based Payment* command for printing purposes.

2-5.9.4 Token Based Payment

Command

By issuing an *Token Based Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

Response

When the PSAM has responded to the *Token Based Payment* command, the application control is returned to the MAD-Handler.

The response to the *Token Based Payment* command will conform to the format defined in section 2-14.6.14 page 2-14-85.

Supplementary Authorization transactions will always require an online connection to the acquirer host.

2-5.9.5 Validate Data

Command

By issuing a *Validate Data 2* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

NOTE: The *Validate Data 2* command may consist of one or two segments depending of the amount of data.

- 2-5.9.5.1 A The *Validate Data 2* command shall conform to the format defined in section 2-14.6.3 page 2-14-59.

Response

See section 2-5.3.5 page 2-5-18

2-5.9.6 Complete Token Based Payment

Command

By issuing a *Complete Token Based Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM. The PSAM may issue commands to the Data Store Handler (e.g. if an offline transaction is performed) and the Merchant Application Handler if logging of transaction data is enabled.

- 2-5.9.6.1 A The *Complete Token Based Payment* command shall conform to the format defined in section 2-14.6.15 page 2-14-87.

Response

The response to the *Complete Token Based Payment* command will conform to the format defined in section 2-14.6.15 page 2-14-87.

NOTE: Requirement 2-5.3.6.3 page 2-5-19 is only relevant if the cardholder is present.

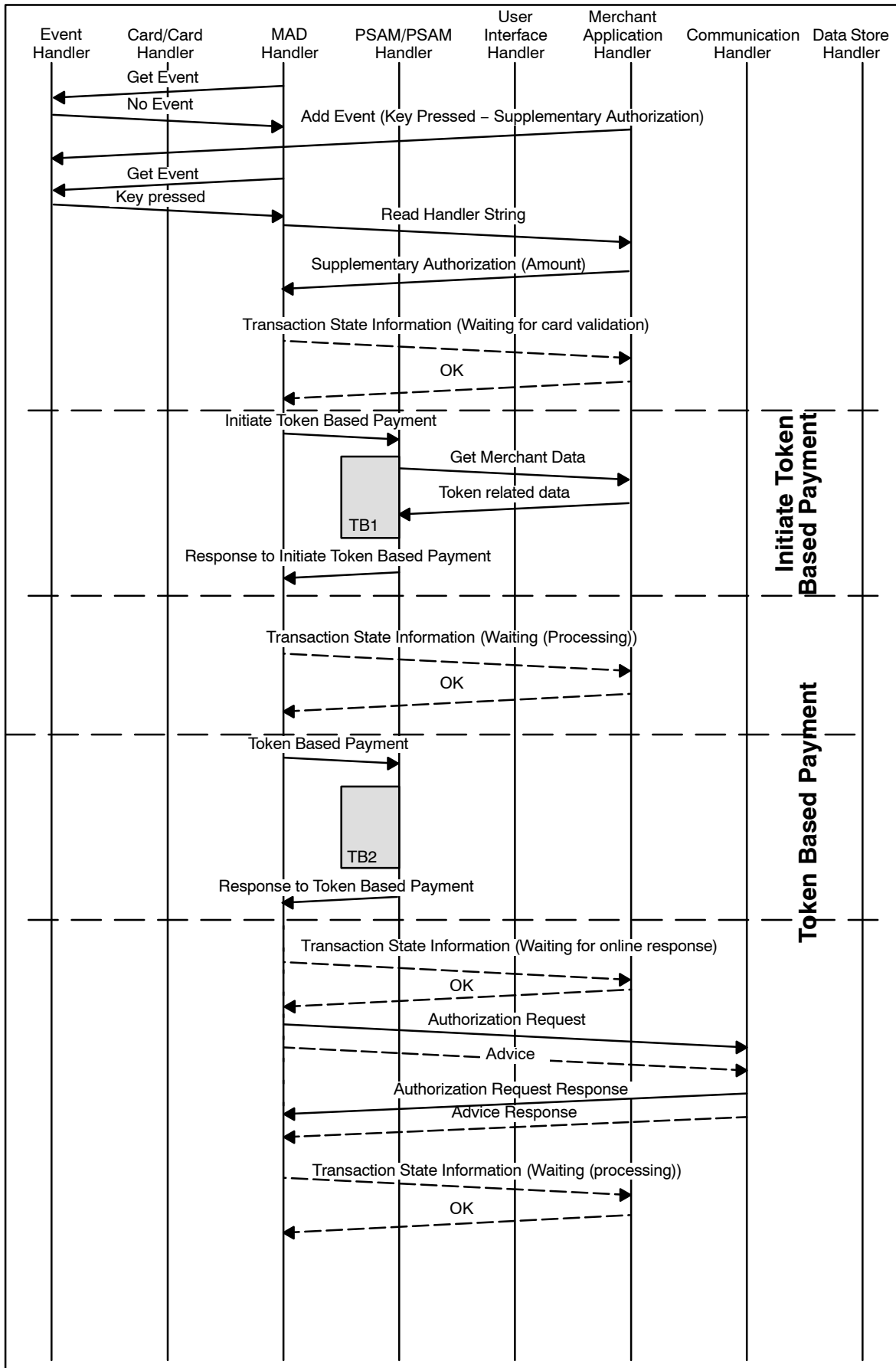


Figure 2-5.24 - Token Based Transaction (Supplementary Authorization - No CVM)

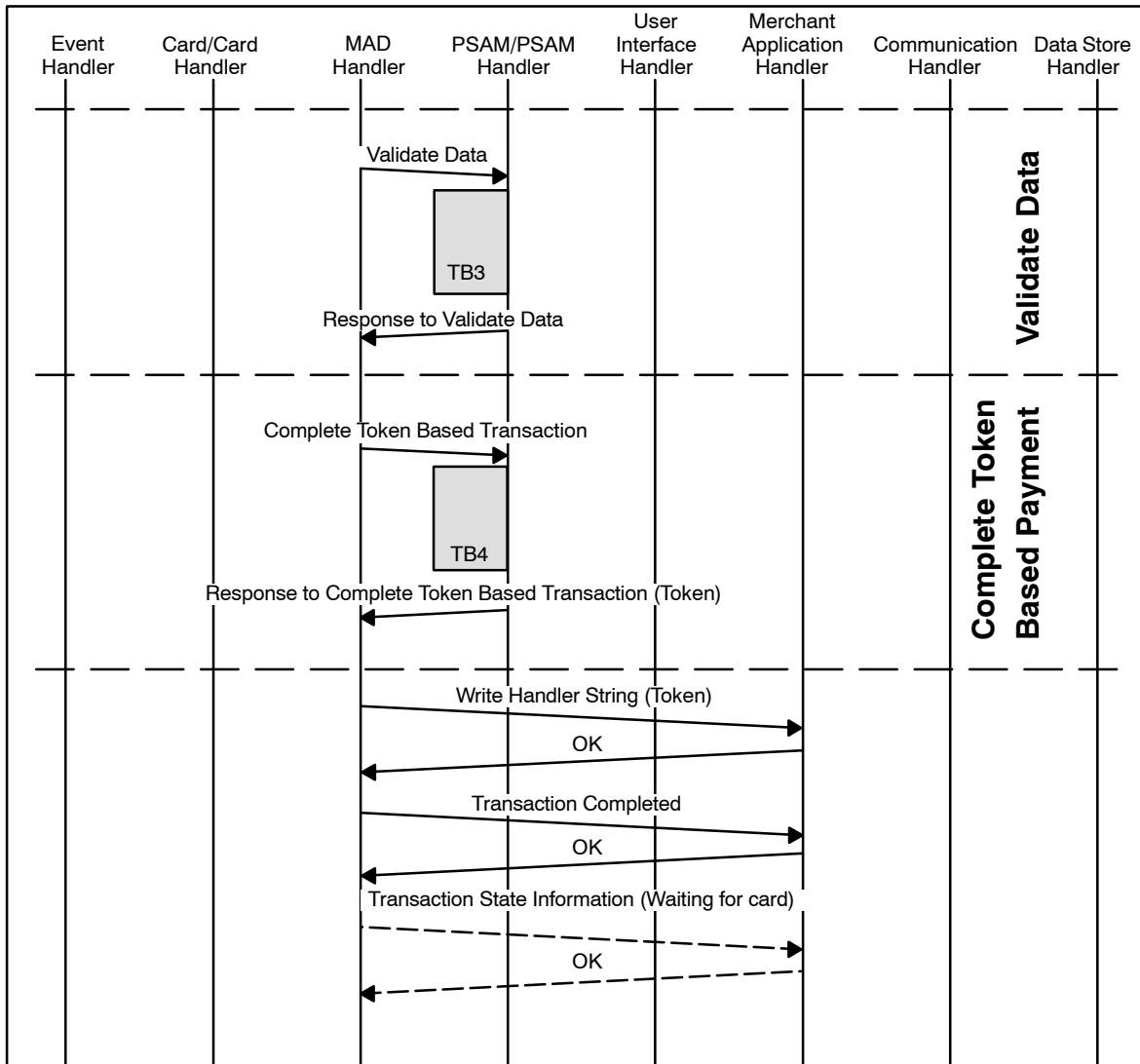


Figure 2-5.24 - Token Based Transaction (Suppl. Authorization - No CVM) (concluded)

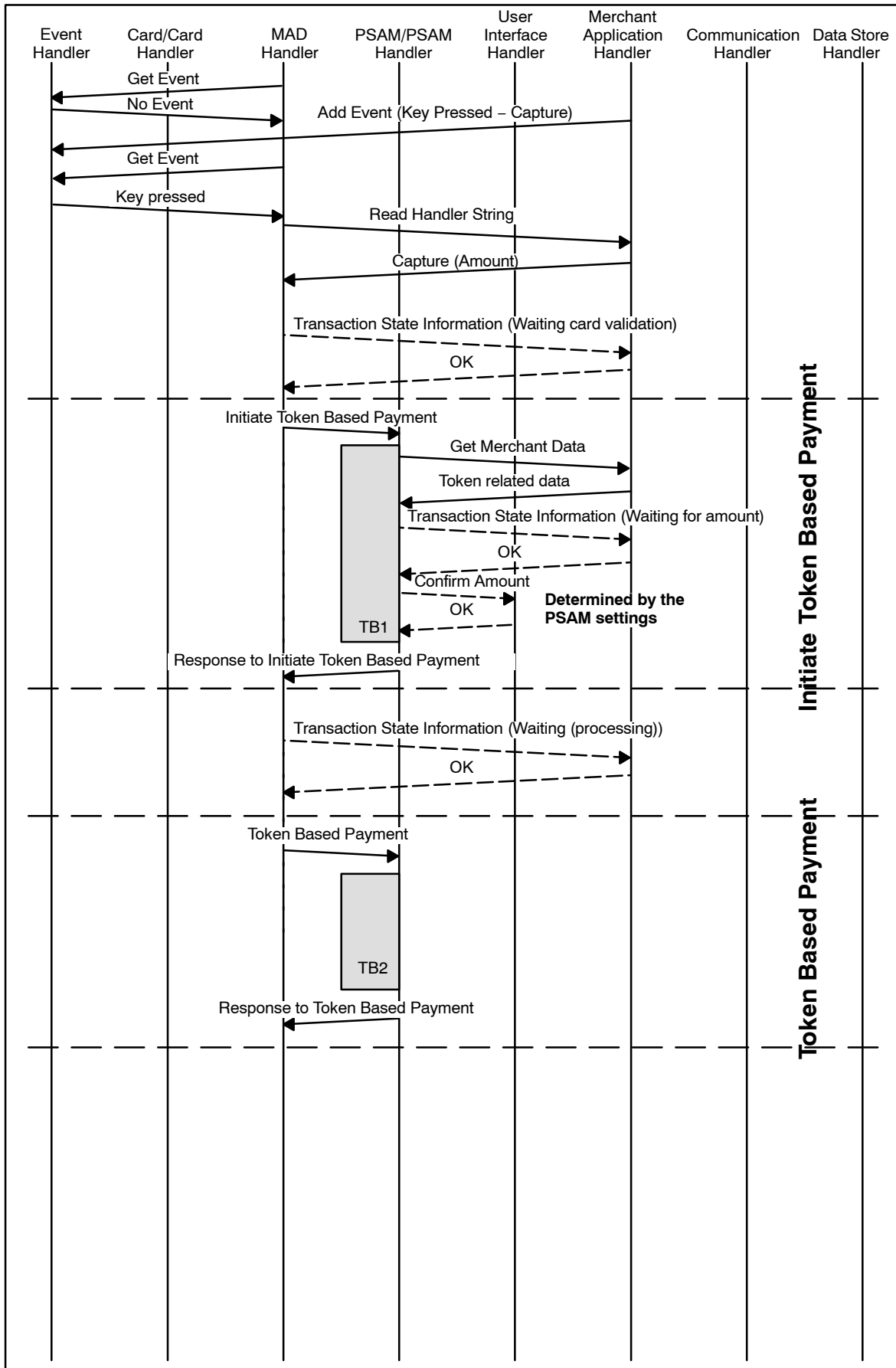


Figure 2-5.25 - Token Based Transaction (Capture - Signature)

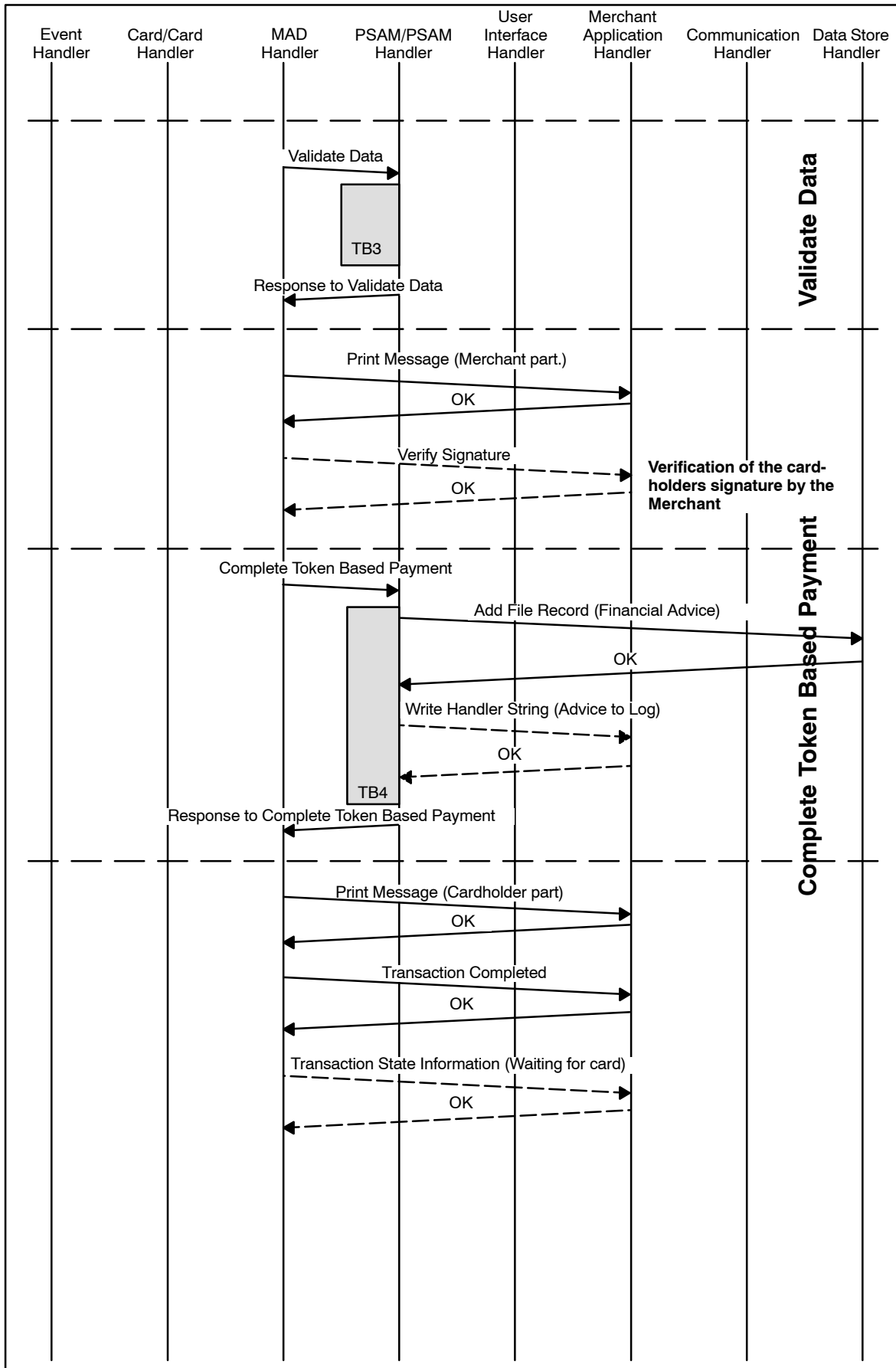


Figure 2-5.25 - Token Based Transaction (Capture - Signature) (concluded)

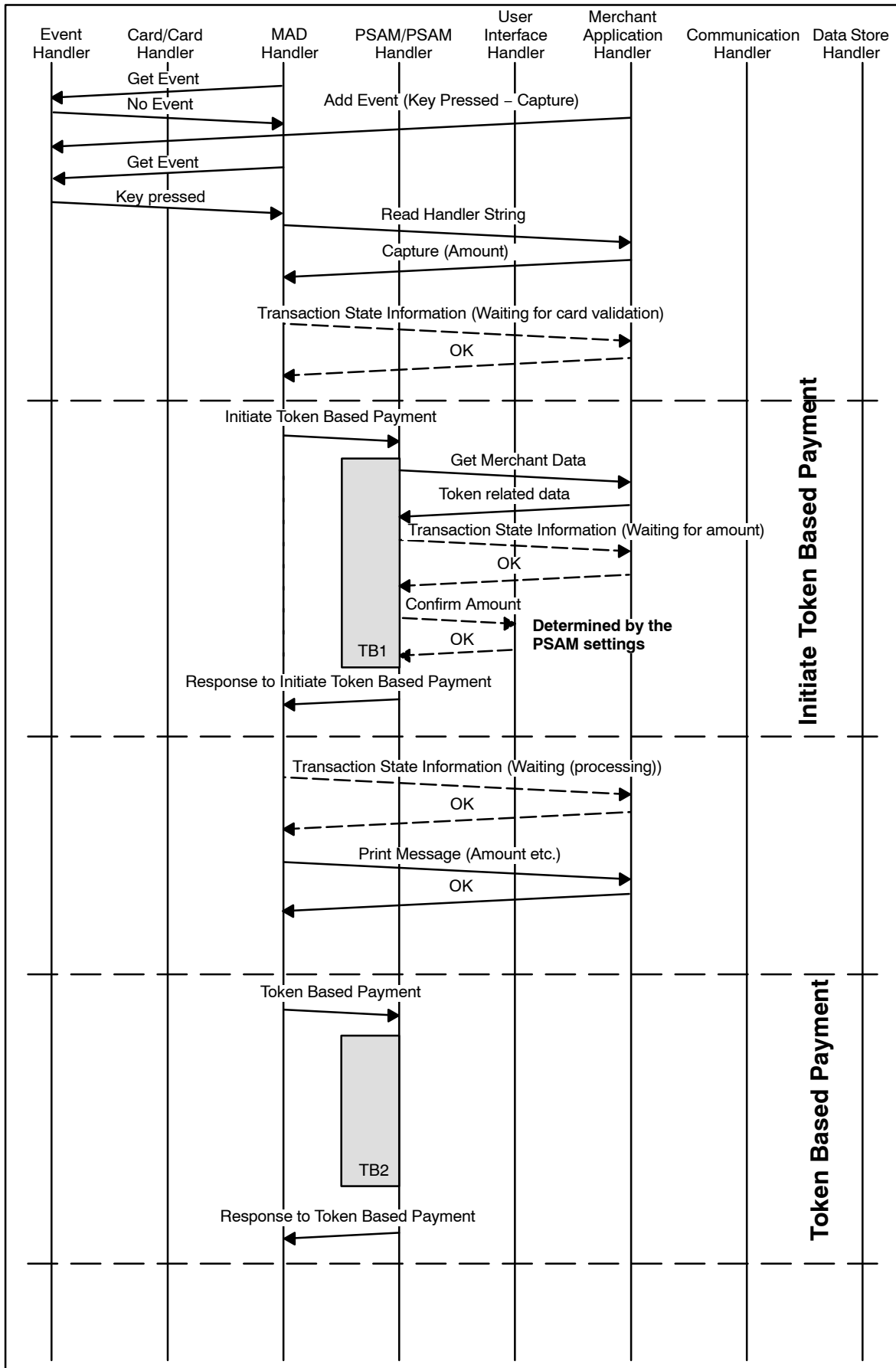


Figure 2-5.26 - Token Based Transaction (Capture - No CVM)

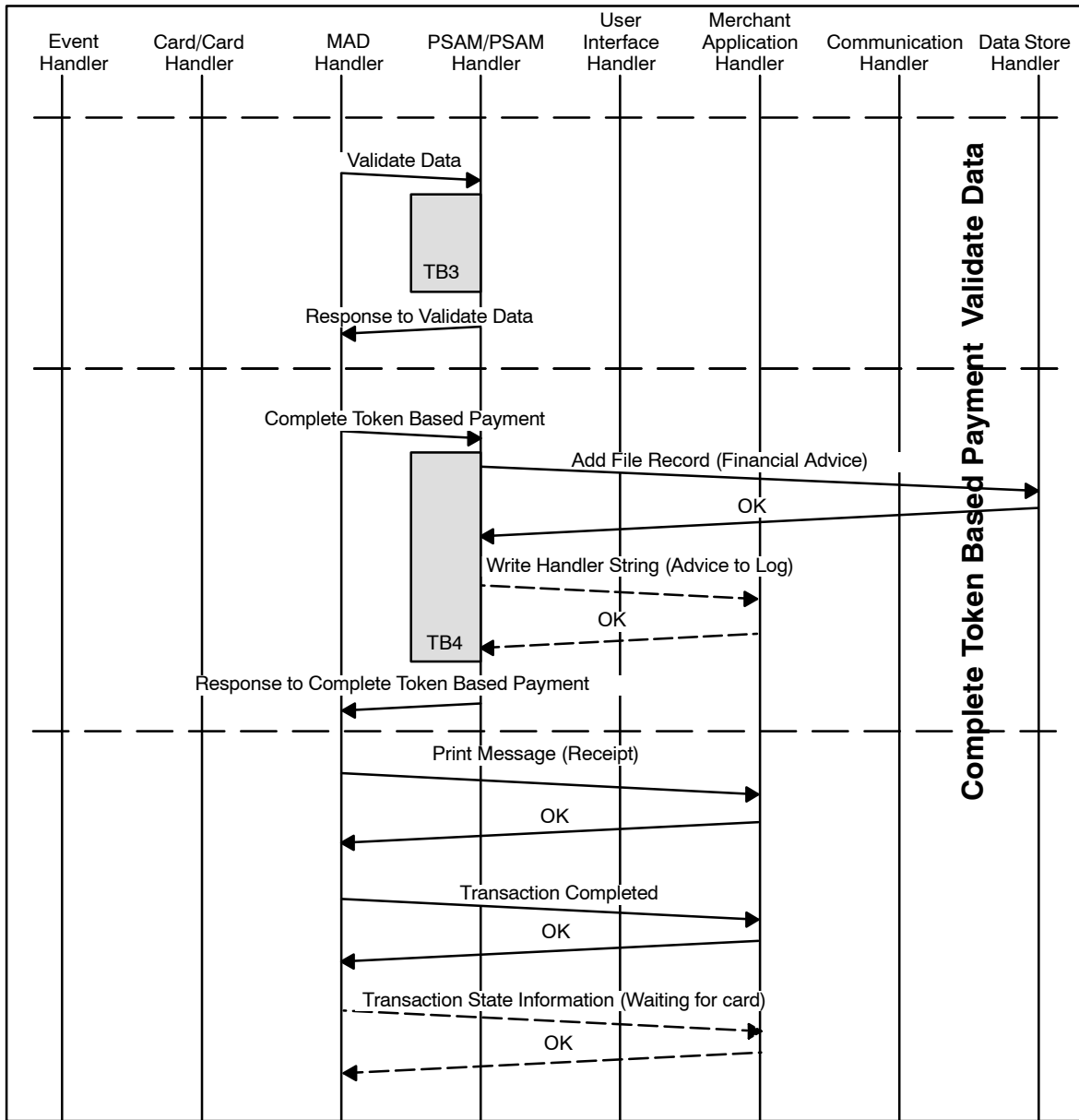


Figure 2-5.26 - Token Based Transaction (Capture - No CVM) (concluded)

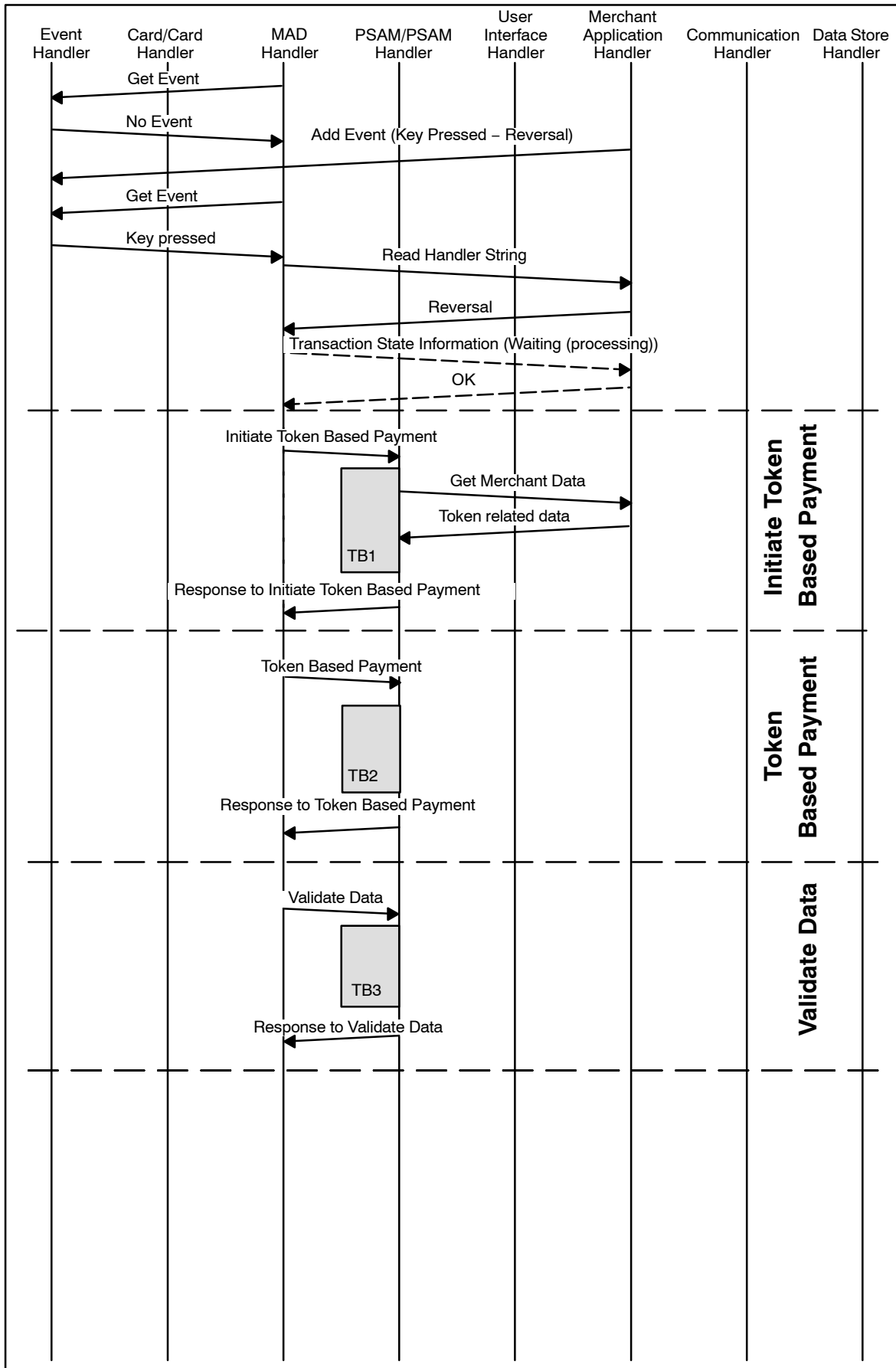


Figure 2-5.27 - Token Based Transaction (Reversal (Authorization) - No CVM)

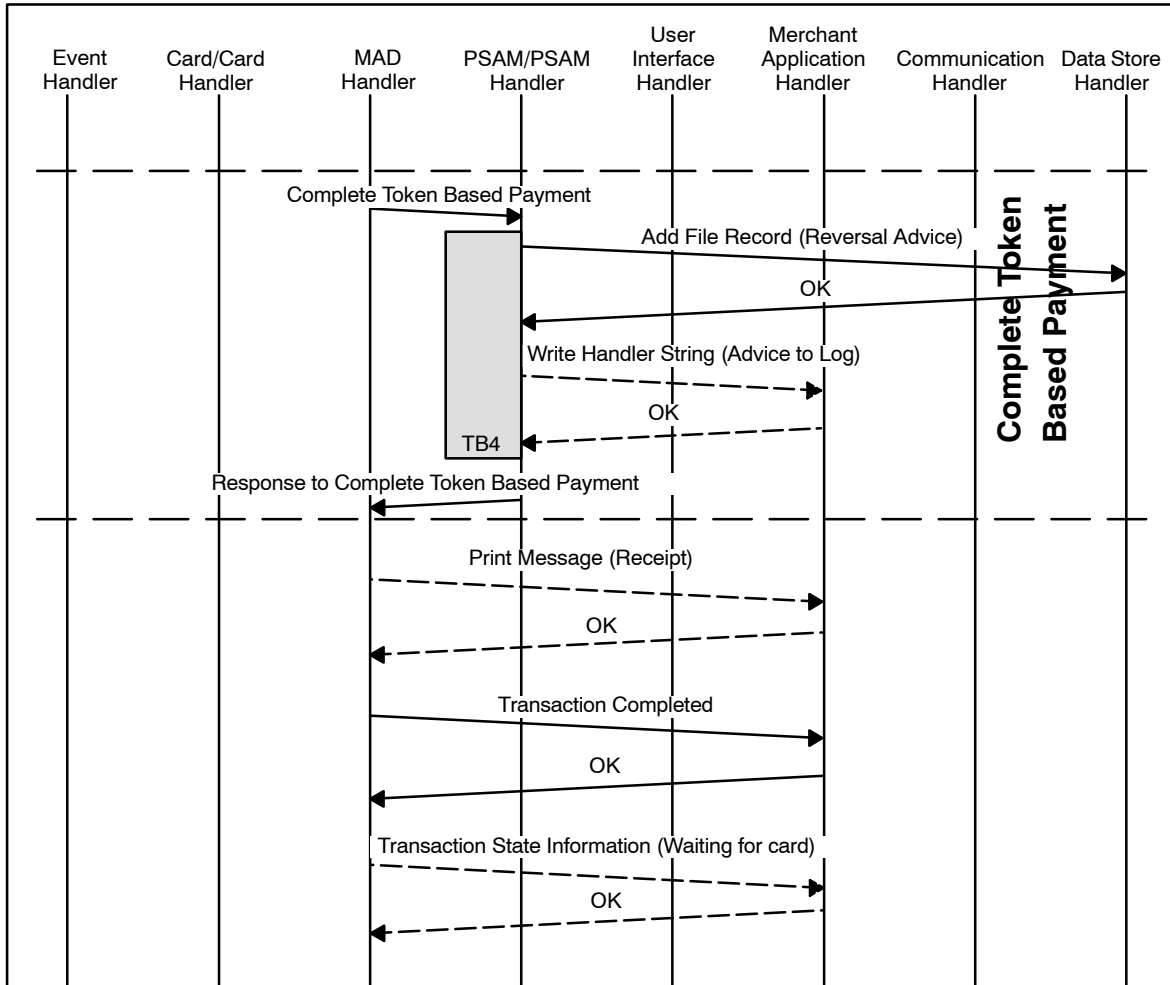


Figure 2-5.27 - Token Based Transaction (Reversal (Authorization) - No CVM) (concluded)

2-5.10 Cancellation

2-5.10.1 Introduction

The Business Call Cancellation is typically utilized in situations where the merchant has entered an incorrect amount and performed a successful purchase transaction before the merchant/cardholder has discovered the mistake. The Business Call may then be used to reverse the most recent purchase transaction.

Whenever a successful purchase transaction is performed, the PSAM stores an image (copy) of the transaction internally. As this image is kept inside the PSAM, a new insertion/swiping of the card or key entering of card data is *not* required when initiating a Cancellation transaction. This ensures that data are not altered during the business call.

2-5.10.2 Transaction Flow

The Business Call Cancellation is divided into the same four steps/commands as the other transaction related Business Calls:

- *Initiate Cancellation Payment*,
- *Cancellation Payment*,
- *Validate Data* and
- *Complete Payment*.

The format of the commands and responses can be found in section 2-14.7 page 2-14-117.

- | | | |
|------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.10.2.1 | A | The terminal shall, in certain regions, support the Business Call Cancellation. |
| 2-5.10.2.2 | A | The terminal shall only enable a Cancellation if the previous Business Call was a successful Purchase transaction. |
| 2-5.10.2.3 | A | The terminal shall only enable a Cancellation for a “revoke” period of 10 minutes after the successful Purchase. |
| 2-5.10.2.4 | C | The terminal may either inhibit the use of Cancellation or generate an error message, if an attempt is made to use the Business Call when not applicable. The error message used shall be message code 'FF', “Invalid transaction” |
| 2-5.10.2.5 | B | The terminal shall, if the previous Business Call was an Authorization, guide the merchant to use the Business Call Reversal of Authorization instead of the Cancellation. |
| 2-5.10.2.6 | A | The terminal shall prompt the merchant for a confirmation before completing the Cancellation transaction. |
| 2-5.10.2.7 | C | The terminal may present information on the Amount and Date & time to the merchant to guide him/her in proceeding with the transaction. |

NOTE: This information is provided by the PSAM in the response to the *Initiate Cancellation Payment* command.

- 2-5.10.2.8 A The terminal shall allow the merchant to interrupt the Cancellation. It shall not be possible to resume an interrupted Cancellation.
- A Cancellation transaction is always performed offline. A successful Cancellation will delete any corresponding Financial Advice stored in the Data Store, and generate a Reversal Advice.
- 2-5.10.2.9 A The terminal shall support the following TAPA commands
- *Get File Record*
 - *Delete File Record*
- These commands are issued by the PSAM during the Cancellation transaction. The *Get File Record* command is used to check if the previously created Financial Advice still is present and valid. The *Delete File Record* command is used to delete the previously created Financial Advice, when all the conditions for performing a Cancellation transaction is fulfilled.
- 2-5.10.2.10 A The terminal shall not autonomously initiate an Advice Transfer, an Advice Enclosing or an Advice Forwarding of the most recent Financial Advice within in the time frame for Cancellation.
- NOTE:** Transferring the most recent Financial Advice will remove the possibility of a Cancellation of that transaction.
- 2-5.10.2.11 A The terminal shall generate a Cancellation receipt when the transaction is successful. The receipt shall contain all of the content of the original receipt. The receipt shall as well contain a "Cancellation indicator" in line TR4.
- 2-5.10.2.12 A The PSAM will not (cannot) return information on Surcharge, Extra and DCC information. The terminal shall thus keep an image of the previous receipt in order to be able to generate an Cancellation receipt.
- 2-5.10.2.13 A The terminal shall not store any of the data previously transferred to the host. The PSAM will take care of this, including any additional "envelope" data.
- NOTE:** It is possible to distinguish a Reversal Advices created as part of Cancellation transaction by the value of the Message Reason Code (MRC). The value of 4005 (Original amount incorrect) indicates that a Cancellation transaction has been performed.
- 2-5.10.2.14 A The terminal shall not generate any receipt, if the Cancellation transaction fails.
- 2-5.10.2.15 A The terminal shall not generate any entry in the Transaction Report, if the original Purchase transaction generated a Financial Advice, and this Financial Advice has not yet been included in the report.
- 2-5.10.2.16 A The terminal shall generate a corresponding entry in the total report, if the original Purchase transaction was an on-line MSC transaction, or if the corresponding Financial Advice already has generated an entry in the total report.

- 2-5.10.2.17 C The information should be stored in a special 'cancellation' group, and not in the 'refund' group, as the handling of a Cancellation transaction will differ from the handling of a Refund transaction.
- NOTE:** A Refund transaction may include a surcharge to be paid by the cardholder in the total amount.
- 2-5.10.2.18 A The terminal shall handle a purchase transaction and a corresponding Cancellation as a voided transaction in the total report.
- The flow for the different elements of a Cancellation transaction is shown in section 2-5.5 page 2-5-23 through 2-5.8 page 2-5-62.

2-5.11 Post Registration

2-5.11.1 Introduction

Post Registration is handled by the two Business Calls:

- Post Purchase
- Post Refund

The Business Calls Post Purchase and Post Refund are typically used *after* a Capture has been performed, if either unexpected expenses arise later or funds are to be returned due to lesser expenses than expected.

When performing either the Post Purchase or Post Refund, the cardholder is typically not present, therefore the required card data are obtained from a Token (EMV, MSC or Key Entered based).

Irrespective upon which Card Data Source the Token is based, the Business Calls Post Purchase and Post Refund will end up as a Key Entered Purchase transaction (No CVM) or a Key Entered Refund transaction (merchant signature requested) respectively.

Post Registration is applicable for Terminal Type 22 (Attended - Offline with online capability) only. See Book 1, table 1-6.2 for further information.

Further introductory information can be found in Book 1, section 1-10.5.7.

2-5.11.2 Transaction Flow

The Business Calls Post Purchase/Post Refund are divided into the same four steps/commands as e.g. for a Capture:

- *Initiate Token based Payment,*
- *Token based Payment,*
- *Validate Data and*
- *Complete Payment.*

The formats of the commands and responses can be found in section 2-14.6.14 page 2-14-85.

- 2-5.11.2.1 A Card Data Source shall be set to '03' (Token).
- 2-5.11.2.2 A When performing the Business Call Post Purchase, the Transaction Request (TR) shall be set to '0A'.
- 2-5.11.2.3 A When performing the Business Call Post Refund, the Transaction Request (TR) shall be set to '0B'.
- 2-5.11.2.4 A When using the Merchant Initiative (MI) the terminal shall not force any CVM.
- NOTE:** It is still possible to force online/offline.
- 2-5.11.2.5 A The terminal shall set the POS Entry Mode to 10000X.
- 2-5.11.2.6 A The Transaction Type (TT) shall be set to '00' (Goods and services) when performing a Post Purchase.
- 2-5.11.2.7 A The Transaction Type (TT) shall be set to '20' (Returns/Refunds) when performing a Post Refund.
- 2-5.11.2.8 A The final amount shall be present when initiating either a Post Purchase or Post Refund.
- 2-5.11.2.9 A Cashback shall not be included for Post Purchase or Post Refund.
- 2-5.11.2.10 A Account Type shall be set to '00' (Default - unspecified) i.e. Account Type Selection is not supported.

2-5.12 Addendum Records

2-5.12.1 Introduction

Addendum Records are applicable when the merchant wish to add information concerning goods and services to a specific financial transaction.

The actual format of the Addendum Record is out of scope for this specification.

Examples of tags for different merchant categories can be found in section 2-13.9.21.

2-5.12.2 Handling of Addendum Records

Pre-conditions

Addendum Records can *only* be attached to successful Captures.

- 2-5.12.2.1 A If an addendum record is going to be attached, the terminal shall indicate it in the data element Merchant Initiative (MI). Merchant Initiative (MI) is part of the *Initiate Payment* command when performing the Capture.

NOTE: More Addendum Records may be attached to one Capture. This is handled by issuing several *Add Addendum Record* commands.

As the data element Merchant Initiative (MI) is conveyed to the host (field 62), the host will expect an Addendum Record message to follow if indicated.

Add Addendum Record Command

- 2-5.12.2.2 A The terminal shall issue an *Add Addendum Record* command to the PSAM immediately after the Capture is performed.

The information given in the *Add Addendum Record* command provides the necessary data for the PSAM to create a complete Addendum Record message (the format can be found in section 2-13.8.7).

NOTE: The *Add Addendum Record* command will cause the System Trace Audit Number (STAN) to be incremented.

- 2-5.12.2.3 A An *Add Addendum Record* command shall always be issued to the same PSAM where the previous financial transaction was performed.

- 2-5.12.2.4 A The length of the Addendum Record is limited to 254 - 55 = 199 bytes. If more data is to be included, an additional addendum record shall be attached. The data element "Addendum Status" shall be adjusted accordingly.

- 2-5.12.2.5 A An additional *Add Addendum Record* command shall succeed the *Complete Payment* command.

Table 2-5.4 describes where the terminal may fetch the data elements required for the *Add Addendum Record* command. Some of these data elements are used to link the addendum record to the previously performed Financial Advice (Capture).

Table 2-5.4 - Source of the Data Elements Included in the *Add Addendum Record* Command

Data Elements	Source
Addendum Status	Terminal/Merchant Application
LEN _{PAN}	Response to <i>Initiate Token Based Payment</i> command
PAN	Response to <i>Initiate Token Based Payment</i> command
Systems Trace Audit Number	Response to <i>Initiate Token Based Payment</i> command
Date, local transaction	Same as in <i>Initiate Token Based Payment</i> command
Time, local transaction	Same as in <i>Initiate Token Based Payment</i> command
MRC	As defined in section 2-13.9.7
Batch Number	Same as in <i>Token Based Payment</i> command
Terminal Identification	Same as in <i>Initiate Token Based Payment</i> command
MAD-Handler ID	Terminal/MAD-Handler
Terminal Approval Number	Terminal/MAD-Handler
LEN _{ADD}	Terminal/Merchant Application
Addendum Record	Terminal/Merchant Application

Complete Payment Command

- 2-5.12.2.6 A The terminal shall send a *Complete Payment* command immediately after the *Add Addendum Record* command in order to clean-up the entry.

In addition, the PSAM will send an *Add File Record* command to the Data Store to store the Addendum Record message before it responds to the *Complete Payment* command.

- 2-5.12.2.7 A Transaction Status shall be set to '00' indicating a successful transaction.

Logging

Irrespective of the value of "Info Level" (conveyed in the *Exchange Debit/Credit Static Information* command), Addendum Records will not be logged (only Financial Advices are logged!).

An example of the command flow between different handlers is depicted in figure 2-5.28.

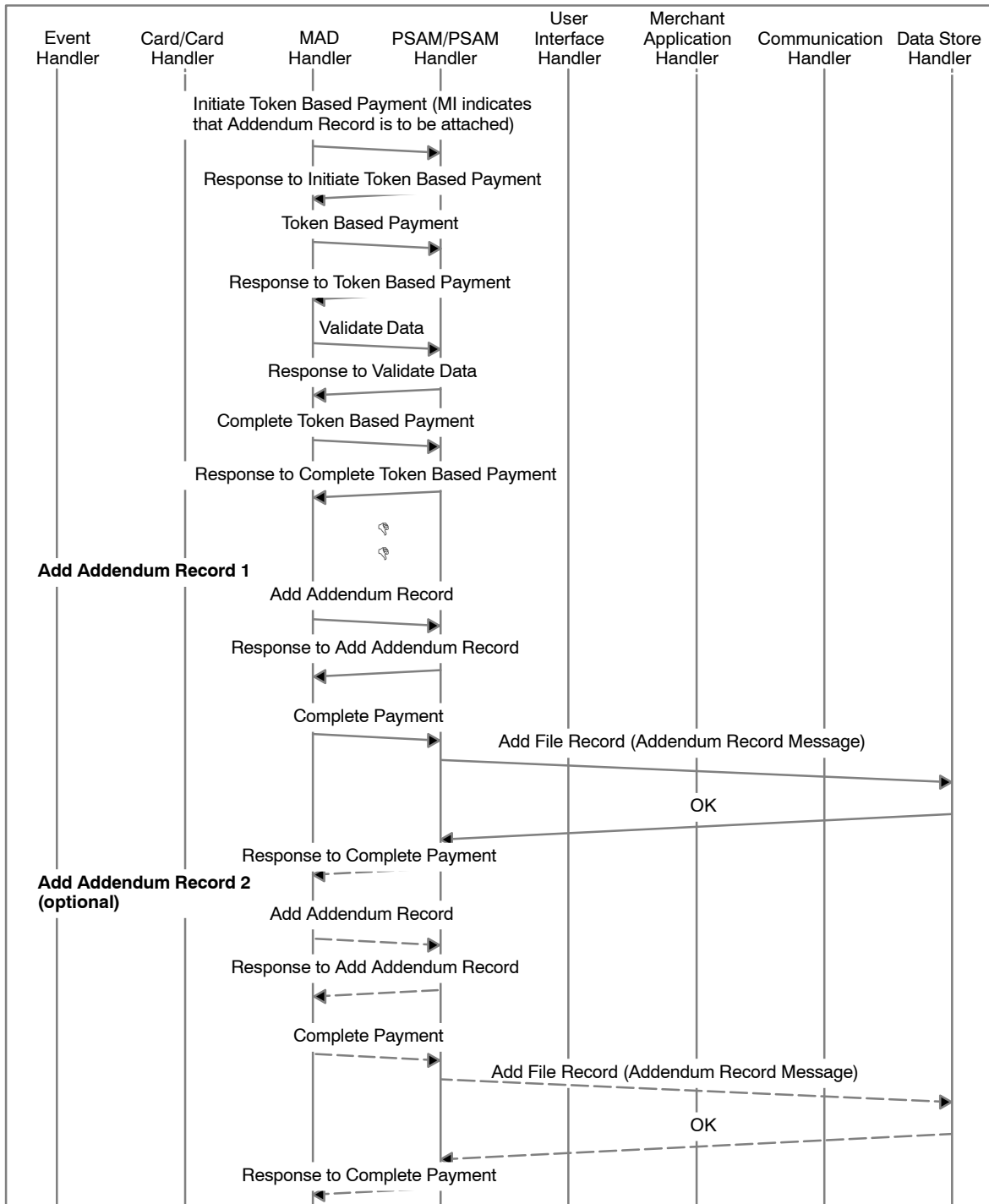


Figure 2-5.28 - Example of Addendum Record Command Flow (Capture)

2-5.13 Administrative Transactions and Processes

2-5.13.1 Introduction

For POS terminals Administrative routines are either initiated by the merchant or initiated automatically. For a UPT terminal, administrative routines are initiated automatically.

For some administrative transactions, the PSAM is involved in the creation of the request or the validation of the host response, see table 2-5.5.

Table 2-5.5 - Administrative Transactions

Transaction	Message request creation		Message request response validation	
	Terminal	PSAM	Terminal	PSAM
Installation		☞		MAC
Advice Transfer	☞		Check value	
PSAM Update	☞			MAC on individual PSAM Updates
PSAM Deactivation		☞		MAC
Clock Synchronization	☞			

Advice Transfer is always initiated by either the merchant, the Merchant Application or the MAD-handler in order to empty the Data Store.

To avoid an accumulation of advices in the Data Store, the terminal is required to continuously transfer advices to the host system according to defined rules, see section 2-5.15 page 2-5-101.

- 2-5.13.1.1 A The MAD-Handler shall be able to identify and interpret the Action Code (result of the transaction) in the host response to administrative messages and advices.

2-5.13.2 Installation Transaction

The purpose of the Installation transaction is to establish a relationship in the host between the terminal and PSAM.

No card related transactions can be initiated before an Installation transaction has been successfully performed.

When the PSAM has been delivered to the merchant, the PSAM might not have been loaded with all the data necessary for performing card related transactions or some of the data loaded might be outdated.

Therefore, a successful Installation transaction is always followed by PSAM Update transaction.

NOTE: Please note that a reverse transaction of the Installation transaction (e.g. De-installation transaction) is *not* defined.

2-5.13.2.1 A An Installation transaction shall be performed according to figure 2-5.29.

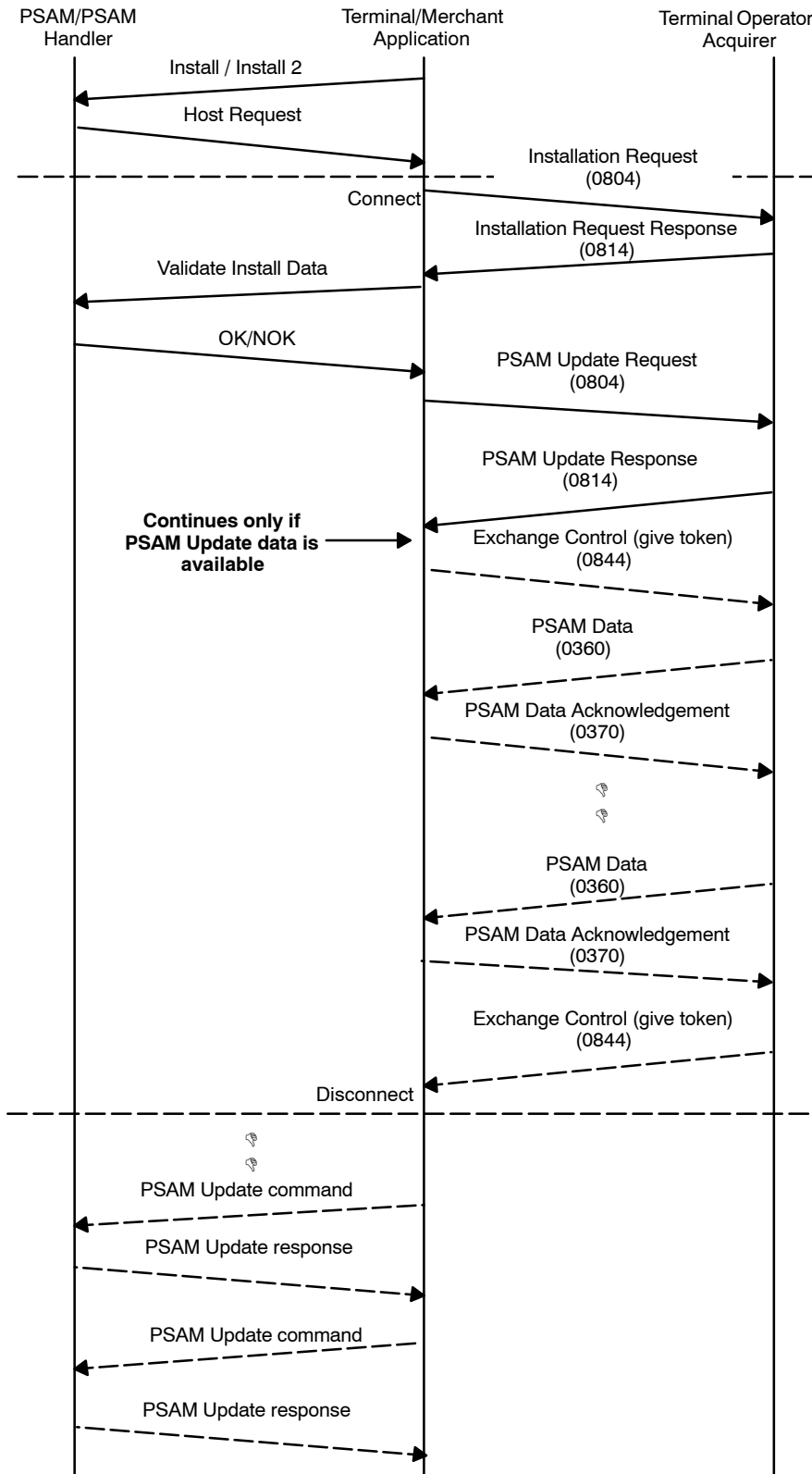


Figure 2-5.29 - Installation Transaction

2-5.13.2.2 A An Installation transaction shall be performed whenever the *Start-up PSAM* or *Exchange Debit/Credit Static Information* command indicates the need for it in the response.

Consequently, the merchant must initiate an Installation transaction whenever a PSAM is physically inserted in a new terminal. See section 2-5.1.4 page 2-5-10 for further details.

- 2-5.13.2.3 A When the merchant initiates an Installation transaction, the MAD-Handler shall provide the following data elements in the *Install / Install 2* command to the PSAM:
- Terminal Capabilities
 - Additional Terminal Capabilities
 - Software Version Number
 - Hardware Version Number
 - Terminal Identification
 - Terminal Approval No.
 - IDSN (MAD Application ID)
 - Terminal Type
 - POS Capability Code
 - Info Level
 - PED Data (if performing Install 2)
 - PCI Data (if performing Install 2)

- 2-5.13.2.4 A The MAD-Handler shall forward the Installation Request Response (without the APACS header) received from the host in the *Validate Install Data* command to the PSAM.

The final result of the Installation transaction will be given in the response to the *Validate Install Data* command.

- 2-5.13.2.5 A A successful Installation transaction shall be followed by a PSAM Update transaction as defined in section 2-5.13.3 page 2-5-93.

The formats for the Installation messages are defined in section 2-14.5 page 2-14-20 and section 2-13.8.10 page 2-13-58.

NOTE: For details of transferring advices to the host, see section 2-5.15 page 2-5-101.

2-5.13.3 PSAM Update Transaction

PSAM updates are required whenever data, keys etc. are outdated or expired or after an Installation/Advice Transfer. The PSAM Update Transaction allows the Terminal Operator to update the merchant's equipment with the latest parameters to ensure proper operation.

The PSAM Update Transaction will initiate the following action: Receive Updates for the PSAM (e.g. Patch downloads)

The way of initiating the PSAM Update transaction is out of scope of this specification.

- 2-5.13.3.1 B The PSAM Update Transaction shall be performed at least once per day. It is recommended to let it follow the Advice Transfer process.
- 2-5.13.3.2 B A daily PSAM Update transaction shall be initiated automatically.
- 2-5.13.3.3 C A PSAM Update transaction may optionally be initiated manually e.g. by a Business Call.
- 2-5.13.3.4 A The message number conveyed in field 27 of the File Action Instruction Acknowledgement ("0370") shall be an echo of the message number given in the File Action Instruction ("0360"). In case of a repeat, the original message number shall be resent.

- 2-5.13.3.5 C The terminal may, if possible, send the PSAM Updates to the PSAM on the fly.
- 2-5.13.3.6 A The terminal shall, if any PSAM Update command(s) are pending send them immediately after the disconnection, see figure 2-5.31, page 2-5-96.
 If the Terminal Operator host is not capable of delivering PSAM Updates due to heavy load, the host may respond with the Action Code "8421" (Rejected, retry, Initiate new connection - deferred, no further details).
- 2-5.13.3.7 A If the Action Code "8421" is indicated in the PSAM Update Response, the terminal shall initiate a new PSAM Update transaction later (either manually or automatically).
- 2-5.13.3.8 A The terminal must forward each available command APDU to the PSAM(s) in the order they were received by the terminal, regardless of the response received to any preceding update command.
- 2-5.13.3.9 A The terminal shall ensure that all PSAM Update Commands received are transferred to the PSAM., even in the case of terminal shutdown.
NOTE: This may require that updates are stored in non-volatile memory, so that any pending updates are sent to the PSAM as part of the start-up process.
- 2-5.13.3.10 A Each command APDU must be forwarded to the PSAM Handler in an "ICC Command" Terminal Message (Message Type '42') as defined in ref.: 27: "TAPA, Application Architecture Specification".

Figure 2-5.30 gives some guidelines how to extract the PSAM Update command from field 63 of the APACS message.

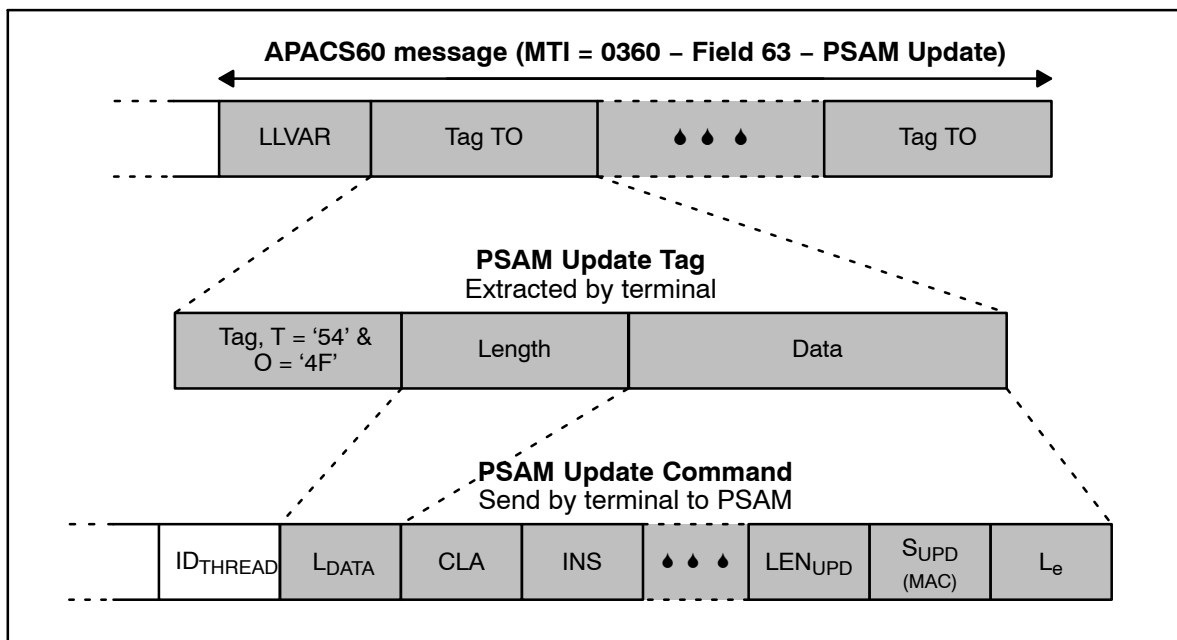


Figure 2-5.30 - Guideline for extracting the PSAM Update Command

- 2-5.13.3.11 A When formatting the terminal message, the terminal Debit/Credit application shall determine the PSAM sub-address from the PSAM Identification.

- 2-5.13.3.12 A When the MAD-Handler assigns a value for the ID_{THREAD} it shall replace the ID_{THREAD} value in the command APDU accordingly.
- 2-5.13.3.13 A In the response to any of the PSAM Update commands, the PSAM may use the ASW1-ASW2 to request that the terminal performs some actions. After processing *all* available PSAM Updates, the terminal must take action prior to initiating any new Debit/Credit transactions. Figure 2-5.39 page 2-5-116 defines the priority when different ASW1-ASW2 are received. Only the highest priority shall be processed.

NOTE: Handling of PSAM updates during the installation sequence is defined in section 2-5.1 page 2-5-1.

If e.g. the PSAM has requested the start-up procedure (ASW1-ASW2 = '1002'), the terminal must complete all outstanding updates and then perform the PSAM start-up procedure.

The formats for the PSAM Update messages are defined in section 2-14.5 page 2-14-20 and section 2-13.8.12 page 2-13-61.

Service Records

A Service Record contains cryptographic check values computed by the PSAM on selected tables that reside in the PSAM itself. The PSAM will create a complete Administrative Advice (Service Record) and store it in the Data Store. When this Administrative Advice is transmitted to the host in an Advice Transfer, it enables the Terminal Operator to centrally monitor vital data (e.g. cryptographic key versions) that reside in the PSAM.

- 2-5.13.3.14 A After sending all PSAM Updates, the terminal shall send a *Create Service Record* command to the PSAM.

NOTE: The PSAM may store Service Records in the terminal Data Store while receiving PSAM Updates, the Create Service Record is sent to the PSAM in order to inform the PSAM that the last PSAM Update has been delivered and that the final Service Record may be created and stored.

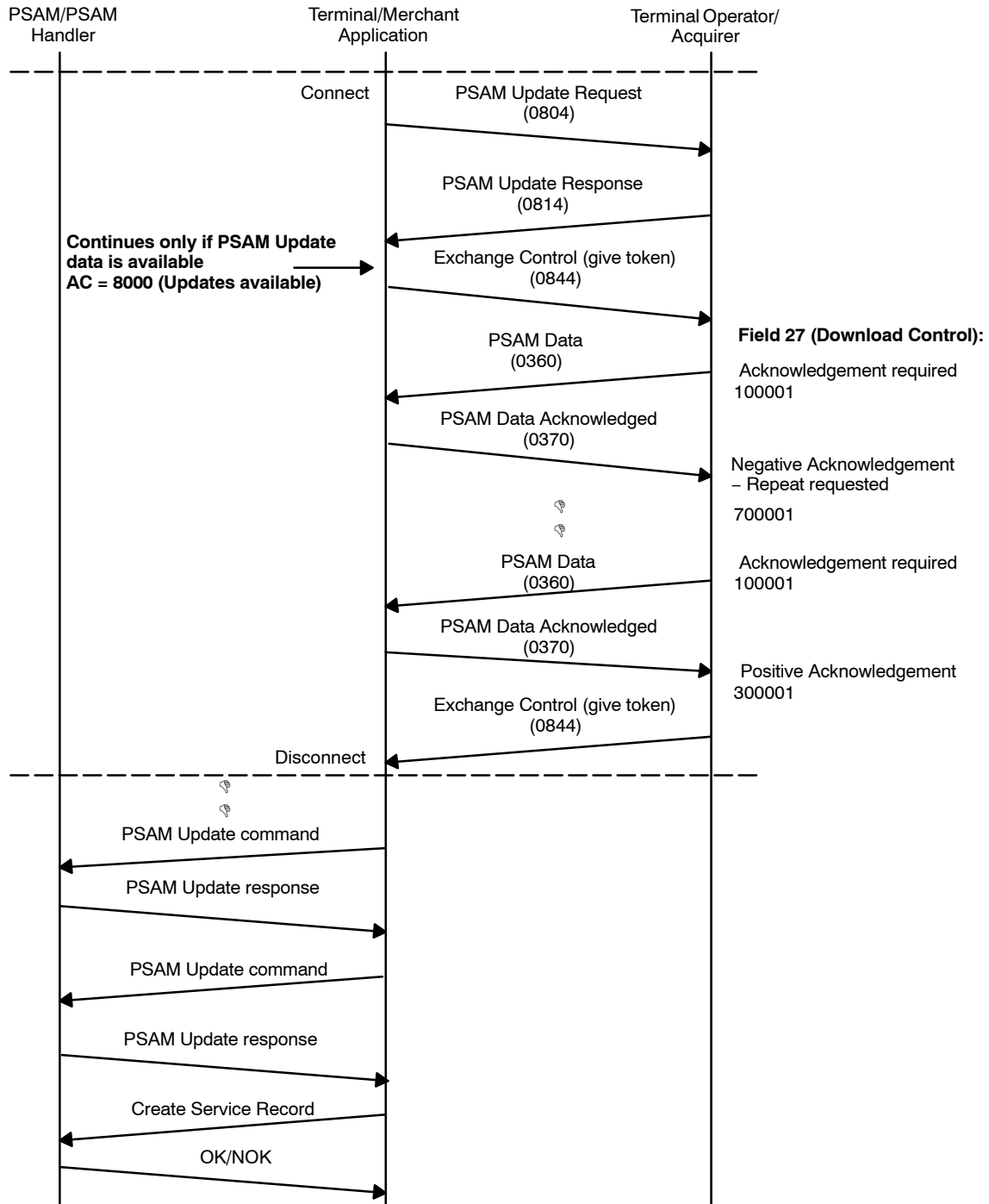


Figure 2-5.31 - PSAM Update Transaction

2-5.13.4 PSAM Deactivation Transaction

The PSAM Deactivation transaction is initiated when the merchant wants to permanently deactivate the PSAM, e.g. if the merchant ceases to accept cards supported by this PSAM.

- 2-5.13.4.1 A The PSAM Update command(s) (conveyed in PSAM Deactivation Response) shall be sent to the PSAM immediately after the disconnection.
- 2-5.13.4.2 C If possible, the terminal may send PSAM Updates to the PSAM on the fly.

The PSAM is not involved in the validation of the PSAM Deactivation Request Response.

The formats for the PSAM Deactivation messages are defined in section 2-14.5 page 2-14-20.

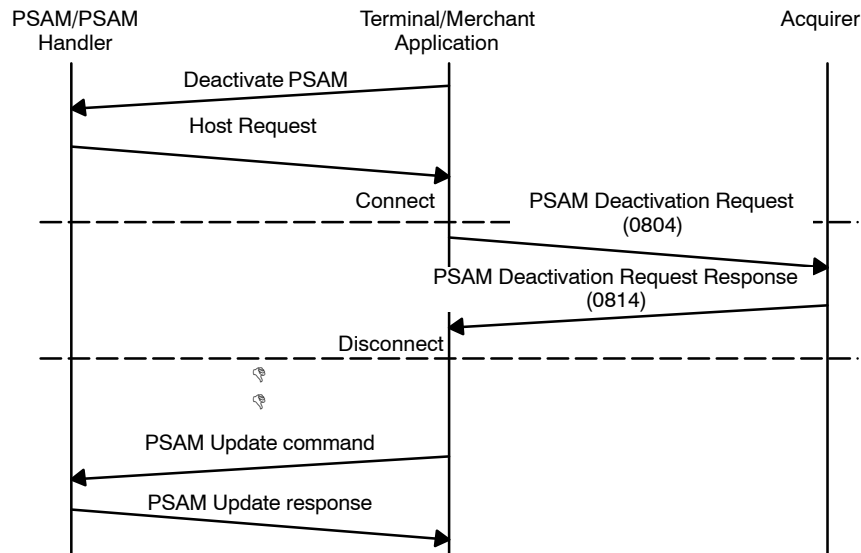


Figure 2-5.32 - PSAM Deactivation Transaction

2-5.13.5 Clock Synchronization

The Terminal Operator host offers a service where the terminal can request a clock synchronization. The way of implementing this feature is out of scope of this specification.

In all Network Management Request Responses (Message Type Identifier 0814), the host time stamp indicated in field 12 and 13 will contain the current time in Copenhagen (Central European Time, CET).

Consequently, the GMT offset in field 15 contains the value '0204' outside the daylight savings time (winter time) and '0408' during the daylight saving time (summer time).

NOTE: The GMT offset for card related transactions contains a fixed value stored in the PSAM at personalization, indicating a time zone. For example, PSAMs intended for the CET zone will use the value '0001'.

The Clock Synchronization Message format is defined in section 2-13.8.9 page 2-13-57.

2-5.14 Online Transactions

This section describes general mechanisms used when communicating with the Terminal Operator host.

All online communication is initiated by the terminal/PSAM.

In this context a Transaction is the complete sequence of events included from an administrative routine or card related Business Call is initiated until the result is known.

A Transaction is initiated by either merchant or cardholder.

A Transaction may include one or more Communication Sessions, but not simultaneously.

2-5.14.1 PSAM Update Flag

The PSAM Update Flag may be included in the APACS header and allows the host to request the terminal to initiate a PSAM Update transaction. An Advice Transfer may also be included.

NOTE: The PSAM Update Flag was previously denoted Advice Request Flag.

The PSAM Update Flag may be present in the headers indicated in section 2-13 page 2-13-1, table 2-13.7 page 2-13-8 Presence of Data Objects in the APACS Header.

2-5.14.1.1 A When the MAD-Handler receives a PSAM Update Flag set in the APACS header, the terminal shall indicate to the merchant/Merchant Application that a PSAM Update transaction shall be initiated.

2-5.14.1.2 C An Advice Transfer may also be included.

NOTE: The terminal shall not be "locked" until a PSAM Update Transaction has been initiated. It is only the message to the Merchant that shall be displayed before any card related transaction may be initiated.

PSAM Update Flag is defined in Section 2-13.7.10 page 2-13-15.

UPT and PSAM Update Flag

2-5.14.1.3 A An UPT shall finish any transactions in progress before performing a PSAM Update transaction.

2-5.14.1.4 A When all transactions in progress have been completed, an UPT shall immediately perform a PSAM Update transaction.

2-5.14.2 PSAM Scripts

The host may decide to transmit PSAM Scripts "directly" to the PSAM without waiting for the terminal to initiate a PSAM Update transaction. The PSAM Scripts will be conveyed in field 63 of a Financial/Authorization Request Response.

As no immediate receipt for PSAM scripts is required, no further action from the terminal is required.

2-5.14.3 Repeat Messages

In case a request or advice message is resent, the Message Type Identifier in the APACS header shall be incremented by one for the first repeat.

Any other modification to the original message and/or to the header will result in a negative response from the host.

NOTE: Repeats are not defined for Network Management Notification, Message Type Identifier = 0844 and File Ac-

tion Instruction Acknowledge, Message Type Identifier = 0370.

- 2-5.14.3.1 A If the terminal does not receive a response to an original request (Message Type Identifier = 0106 & 0206), the terminal shall "mark" the message to indicate repeat before sending the request again.
- NOTE:** In all subsequent sendings the request shall indicate repeat.
- 2-5.14.3.2 A If the terminal does not receive a response after having sent an advice, the terminal shall "mark" the advice to indicate before sending the advice again.

2-5.14.4 Communication Session

Each time the terminal wants to send messages to the host systems, the terminal is going to initiate a Communication Session.

In this context a Communication Session is defined as the procedure for transferring a number of connected messages to or from a terminal.

The number of messages transferred during a Communication Session is not limited.

A Communication Session defines the steps from the terminal initiates the transfer until this session is either closed intentionally or interrupted unintentionally.

If the Terminal does not terminate the Communication Session correctly, the Terminal Operator may terminate the Communication Session, without any notification. The Terminal Operator may deny all attempts to connect to the access points for a given time interval before connection attempts again will be accepted.

Section 2-13.3 page 2-13-2 defines the communications networks and protocols supported.

- 2-5.14.4.1 A If the processing in the terminal indicates that exchange of messages is going to be performed and no Communication Session is ready for use, the terminal shall initiate a new Communication Session.
- 2-5.14.4.2 C If the processing in the terminal indicates that exchange of messages is immediately coming, the terminal may initiate a Communication Session in advance and before any messages are available.
- 2-5.14.4.3 A In case a switched/dial-up communication network is used (e.g. PSTN, ISDN or GSM), the physical line shall be established when a Communication Session is initiated.
- 2-5.14.4.4 A In case a switched/dial-up communication network is used (e.g. PSTN, ISDN or GSM), the physical line shall be cut off when the Communication Session is closed.
- 2-5.14.4.5 A TCP connection shall be established when a Communication Session is initiated.
- 2-5.14.4.6 A The TCP connection shall be closed when the Communication Session is closed.

- 2-5.14.4.7 A During a Communication Session the messages exchanged shall be transferred in an even flow without unnecessary delays.
- 2-5.14.4.8 A The terminal shall be able to detect if an open Communication Session is interrupted unexpectedly.
- 2-5.14.4.9 B If there are no outstanding responses and nothing waiting on queue to be transmitted, the Terminal shall terminate the Communication Session at once.
- NOTE:** No Communication Session shall remain open when not in use.
- 2-5.14.4.10 B Any time-out procedures, intended to detect that opening of a Communication Session is not possible, shall be adapted to the type of communication networks used.
- NOTE:** The time-out value necessary to detect that connection is not possible may e.g. be much shorter for ADSL compared to PSTN network.
- 2-5.14.4.11 A If there are outstanding responses and no activity on the Communication Session for 30 seconds, the Terminal shall terminate the Communication at once.
- NOTE:** The host systems is not going to interrupt an open session, if the host systems are informed of any outstanding responses to the terminal.
- 2-5.14.4.12 A When a time-out is detected the terminal shall interrupt the Communication Session.
- NOTE:** If other responses are outstanding, the terminal shall await all responses or time-outs before closing the session.

2-5.14.5 Terminal Operator Communication Access Points

To be able to offer the highest level of availability, the Terminal Operator may support more than one access point. Each access point has its own IP address and in case a switched network is used, each access point has its own dial-up number too.

A transaction may be initiated by either a Business Call or administrative routines.

- 2-5.14.5.1 A The terminal shall be able to initiate Communication Sessions to at least two different access points.
- 2-5.14.5.2 A If a Communication Session has been interrupted before the actual Transaction has completed, the terminal shall initiate a second Communication Session to one of the other supported access points in order to complete the transaction sequence.
- 2-5.14.5.3 A The terminal shall distribute Communication Sessions to the supported access points evenly, intended to consider an even load on all the access points supported.
- NOTE:** Load distribution may be implemented by simply alternating the first Communication Session between

one of the supported access points, or it could be pseudo-randomly decided per transaction.

2-5.15 Transferring Advices

2-5.15.1 General Principles

Introduction

The general principles for emptying the terminal Data Store are:

- The terminal empties the first file before proceeding to the second file which must be emptied before proceeding a.s.o.
- The terminal has only one advice outstanding at a time, i.e. the response must be received before the next advice is transferred.
- The terminal sends, except as stated below, advices as soon as possible.
- Terminals supporting Cancellation does not send the last stored advice (with MTI 0226) before a number of minutes have passed or before another transaction is performed whichever comes first.

2-5.15.2 The Transfer of Advices

Introduction

One general mechanism is defined for transfer of advices from the terminal Data Store to the host systems:

- Advice Transfer

Advice Transfer is utilized to empty the Data Store completely at a given time. The Advice Transfer is initiated by either the merchant or the Merchant Application.

Online capable terminals will be able to send advices without performing an Advice Transfer.

General Requirements

- | | | |
|------------|---|----------------------------------------------------------------------------------------------------------------------|
| 2-5.15.2.1 | A | The terminal shall support Advice Transfer. |
| 2-5.15.2.2 | A | It shall, on an attended terminal, be possible to manually initiate an Advice Transfer. |
| 2-5.15.2.3 | A | If the Data Store contains any advices, Advice Transfer shall be possible, even though no active PSAM is accessible. |
| 2-5.15.2.4 | A | A UPT terminal shall be able to automatically initiate an Advice Transfer. |
| 2-5.15.2.5 | A | When transferring advices to the host systems, the terminal shall send advices according to the priority order: |

1. File 1 (some Reversal Advices (0426))
2. File 2 (Financial Advices (0226))
3. File 3 (Authorization/Reversal Advices (0126, 0426))
4. File 4 (Administrative Advices (0624) e.g. Service Records and Addendum records)

i.e. the terminal must empty File 1 file before the terminal empties File 2 before etc.

- 2-5.15.2.6 A The terminal shall send the oldest records from a file first.
For handling exception conditions, see section 2-5.15.7 page 2-5-110 and 2-5.15.8 page 2-5-111.

NOTE: Please note requirement 2-5.15.2.8 page 2-5-102.

- 2-5.15.2.7 B The terminal shall process the transfer of advices as a 'background job' not delaying the actual online transaction.

NOTE: If it is not possible to process a transaction without delay while simultaneously transferring advices, the transfer of advices should take place after the processing of the transaction has been completed.

Online Capable Terminals

- 2-5.15.2.8 A The terminal shall, except as specified in requirement 2-5.15.2.9, send all advices as soon as possible after the advice has been stored. The advices shall be sent in the order of the file priority and with the oldest entries first.

NOTE: Please note requirement 2-5.15.2.5

- 2-5.15.2.9 A The terminal shall, if Cancellation is supported, store the latest Financial Advice for up to X minutes. The terminal shall send this stored Financial Advice if a new transaction is initiated or an Advice Transfer is initiated.

This time-out X is the time-span in which it will be possible to perform a Cancellation when no new transaction have been initiated. See section 1-10.2.8, "Cancellation" page 1-10-7.

NOTE: If time-out is reached at the same time as a transaction is initiated, the initiated transaction has priority.

- 2-5.15.2.10 A The time-out X shall be configurable and have a maximum value of 10 minutes. The default value shall be 10 minutes.

- 2-5.15.2.11 B If a transaction initiated results in an online request, the terminal shall send any stored advice together with the request or immediately after the request response has been received.

NOTE: Please note requirement 2-5.15.2.5

- 2-5.15.2.12 B A connection to the host systems shall only be established when relevant.

Offline Only Terminals

These terminals can only transfer advices when performing Advice Transfer.

2-5.15.2.13 A When performing Advice Transfer, the terminal shall send advices in the priority indicated in requirement 2-5.15.2.5 page 2-5-101.

2-5.15.2.14 A When performing Advice Transfer, the terminal shall send the advices one at a time.

Figure 2-5.33 and 2-5.34 each shows an example of a transfer of advices.

Terminals using Dial-up

These terminals need only transfer advices when performing Advice Transfer or when already online in connection with e.g. a financial request.

Terminals supporting Prepaid MSC

When no response is received for an online request, e.g. a 0206, the PSAM will store a Reversal Advice, 0426, in the terminal Data Store.

2-5.15.2.15 A The terminal shall, if no response is received from the Host in response to the original request, send a repeat of the request.

2-5.15.2.16 A The terminal shall, if no response is received from the Host on the repeat request, classify the transaction as not successful. The PSAM will then store a Reversal Advice in the terminal Data Store.

2-5.15.2.17 A Whenever no response is received for an online request, i.e. neither for the original nor the repeat, the terminal shall, after the Complete Payment command have been completed, automatically attempt to transfer the generated advices.

2-5.15.2.18 A The terminal shall at least try to transfer any advices stored in files 1 through 4.

2-5.15.2.19 A The automatically initiated attempt of a transfer of advices shall take place before any new transaction can be initiated from the terminal/cash register.

The Advice Transfer may or may not complete successfully.

2-5.15.2.20 C It is preferable if the terminal initiates a new connection when performing the transfer of advices, i.e. the terminal does not utilize the connection already established but generates a new connection for the transfer of advices.

2-5.15.2.21 A The terminal shall adjust the message type indicator as repeats for requests and advices as required generally, e.g. if a request is resent, it shall be "marked" to indicate a repeat.

2-5.15.2.22 A Any time-out defined between the terminal and cash register for a business call shall take into regard the worst case scenario with regards to no online response.

Examples of a transfer of advices

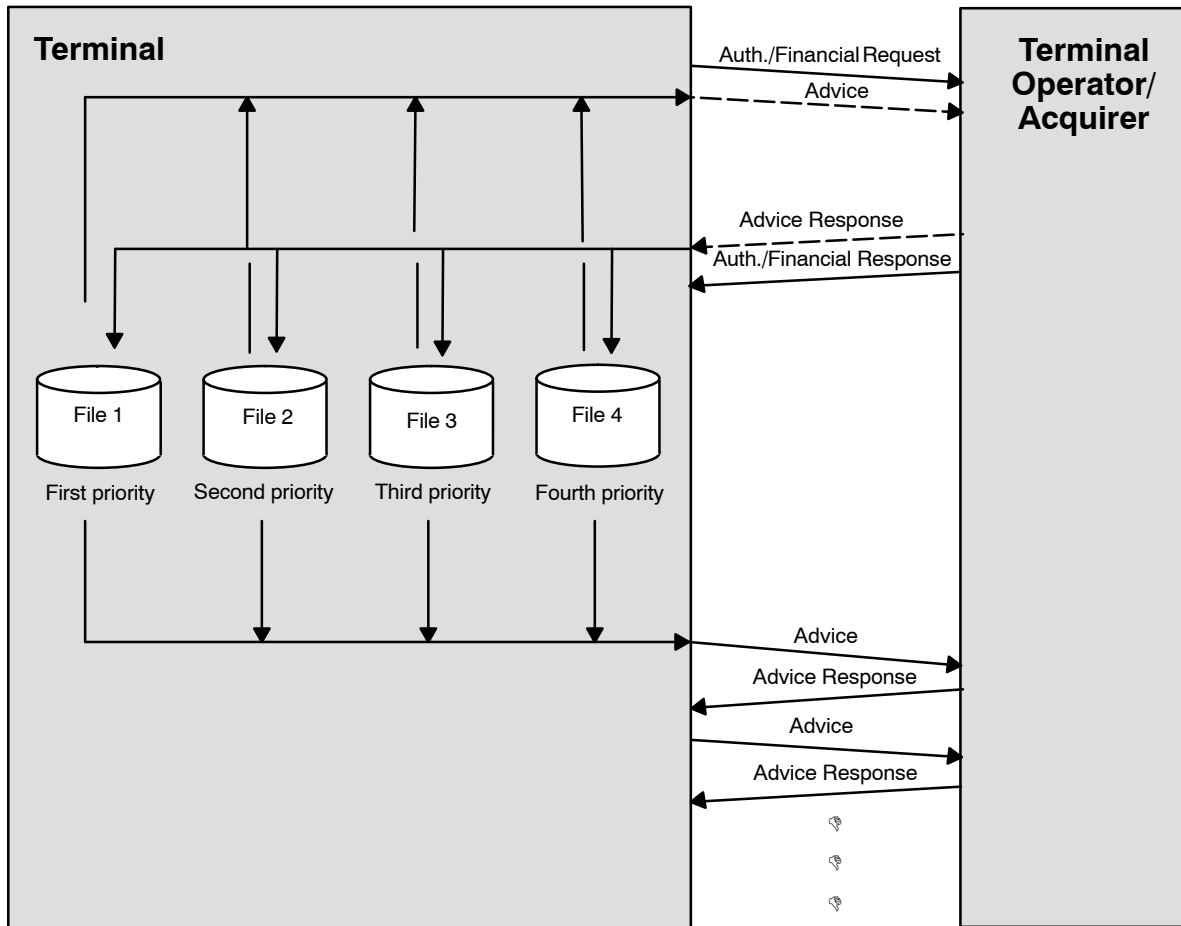


Figure 2-5.33 - Transfer of advices, example 1

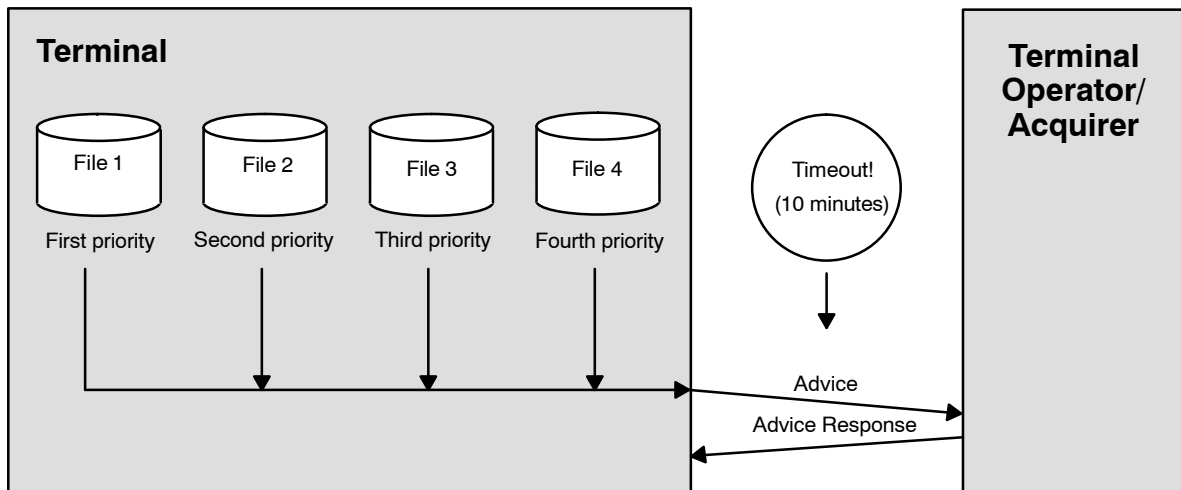


Figure 2-5.34 - Transfer of advices, example 2

2-5.15.3 Advice Transfer

The purpose of the Advice Transfer is to allow the merchant to deliver the advices stored in the Data Store to the Terminal Operator. If the terminal also sends a PSAM Update Request afterwards, any PSAM Updates available are also retrieved.

- 2-5.15.3.1 C Advice Transfer may be initiated by the terminal itself or, if relevant, via a function implemented in the cash register.

Figure 2-5.34 shows the function of the Advice Transfer

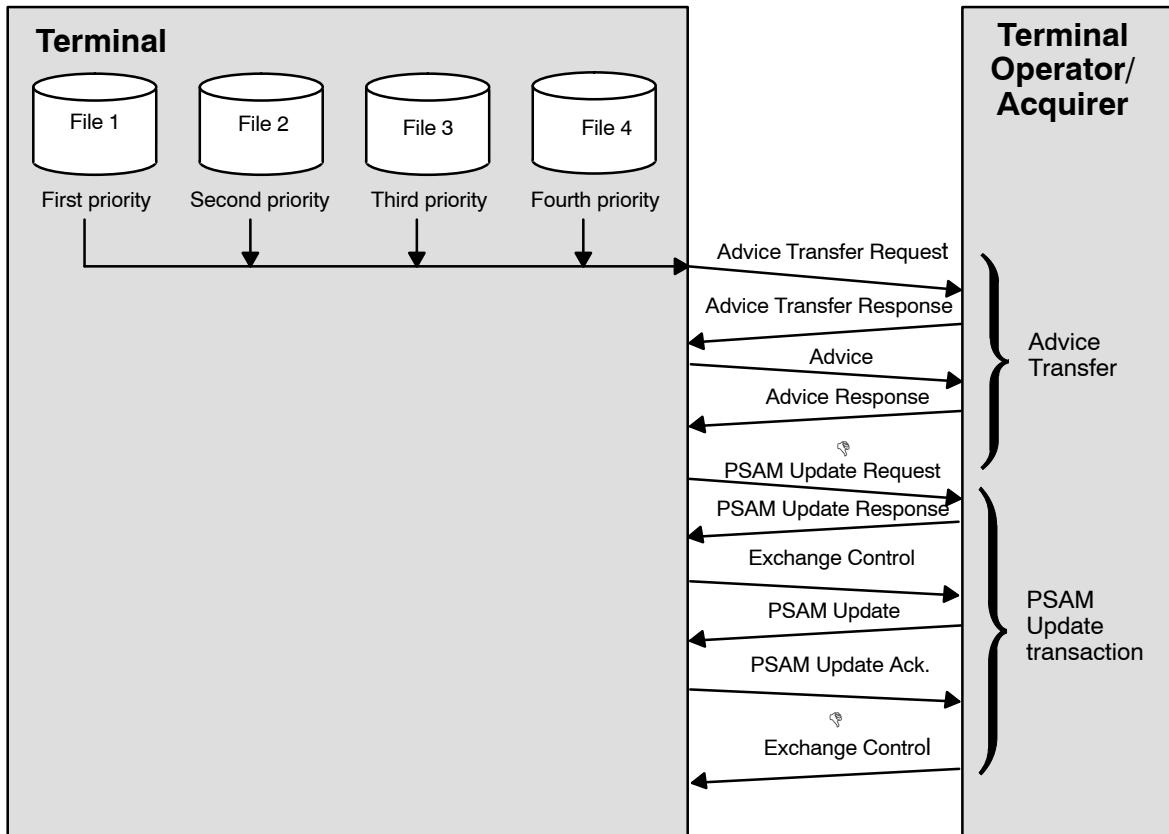


Figure 2-5.35 - Advice Transfer

- 2-5.15.3.2 A When performing Advice Transfer all advices from File 1, File 2, File 3 and File 4 shall be sent to the host systems in the priority stated in requirement 2-5.15.2.5 page 2-5-101.

- 2-5.15.3.3 A Having initiated an Advice Transfer procedure, the terminal shall first send the Advice Transfer Request and await the Advice Transfer Request Response.

NOTE: The formats for the Advice Transfer messages are defined in section 2-13.8.11 page 2-13-60.

- 2-5.15.3.4 A The terminal shall not send any advices with the Advice Transfer Request.

- 2-5.15.3.5 A When the Advice Transfer Request Response has been received, the terminal shall start sending advices dependent upon the value of the received Action Code.

NOTE: Only Action Codes in the range 8000 - 8005 indicates that the Advice Transfer procedure may continue.

If the Terminal Operator host is not capable of receiving advices due to heavy load, the host may respond with the Action Code "8421" (Failed, retry, Initiate new connection - deferred, no further details).

- 2-5.15.3.6 A If the Action Code "8421" is indicated in the Advice Transfer Response, the terminal shall initiate a new Advice Transfer later (either manually or automatically).

- 2-5.15.3.7 A The terminal shall carry on sending advices (if present in the Data Store) as indicated in the Terminal Advice Window Size.
- 2-5.15.3.8 C When all advices have been processed, the terminal may send a PSAM Update Request and await the PSAM Update Request Response.

When performing a settlement, it is recommended to perform an Advice Transfer first as this ensures that all advices have been sent and as the Batch Numbers and counters may be adjusted at this time.

See section 2-5.13.3 regarding the PSAM Update transaction.

For exception handling during Advice Transfer, see section 2-5.15.8 page 2-5-111 Exception Conditions and section 2-5.16.14 page 2-5-124, Action Codes.

2-5.15.4 Security Mechanism

As the PSAM is not engaged in the validation of the Advice Response, an additional security mechanism is applied to prevent accidental loss of data, see figure 2-5.36 page 2-5-107.

The PSAM will generate a random number that will be conveyed in field 61 of the advice. Except for the APACS Header, Advices in Data Store are enciphered.

Furthermore, the PSAM will compute a check value on 8 bytes which will be attached at the end of the advice stored in the Data Store.

- 2-5.15.4.1 A The check value stored in the Data Store shall *not* be part of the advice sent to the host.
- The random number (generated by the PSAM) will be returned in the advice response (field 61) in plaintext.
- 2-5.15.4.2 A The MAD-Handler shall re-compute a new check value using the random number from the advice response as input.
- 2-5.15.4.3 A The algorithm used to compute the check value shall be SHA-1, according to ref. 19: "Secure Hash Standard", where the 8 most significant bytes are used as the check value.
- 2-5.15.4.4 A The MAD-Handler shall delete the corresponding advice stored in the Data Store when both of the following conditions are fulfilled:
- The check value computed by the PSAM and previously stored in the Data Store matches the check value computed by the MAD-Handler,
 - The Action Code is in the range 8000 - 8005 (Accepted).
- 2-5.15.4.5 B The MAD-Handler shall calculate the check value on the fly using the random number from the advice response and, if the check values match, delete the corresponding advice in the Data Store.

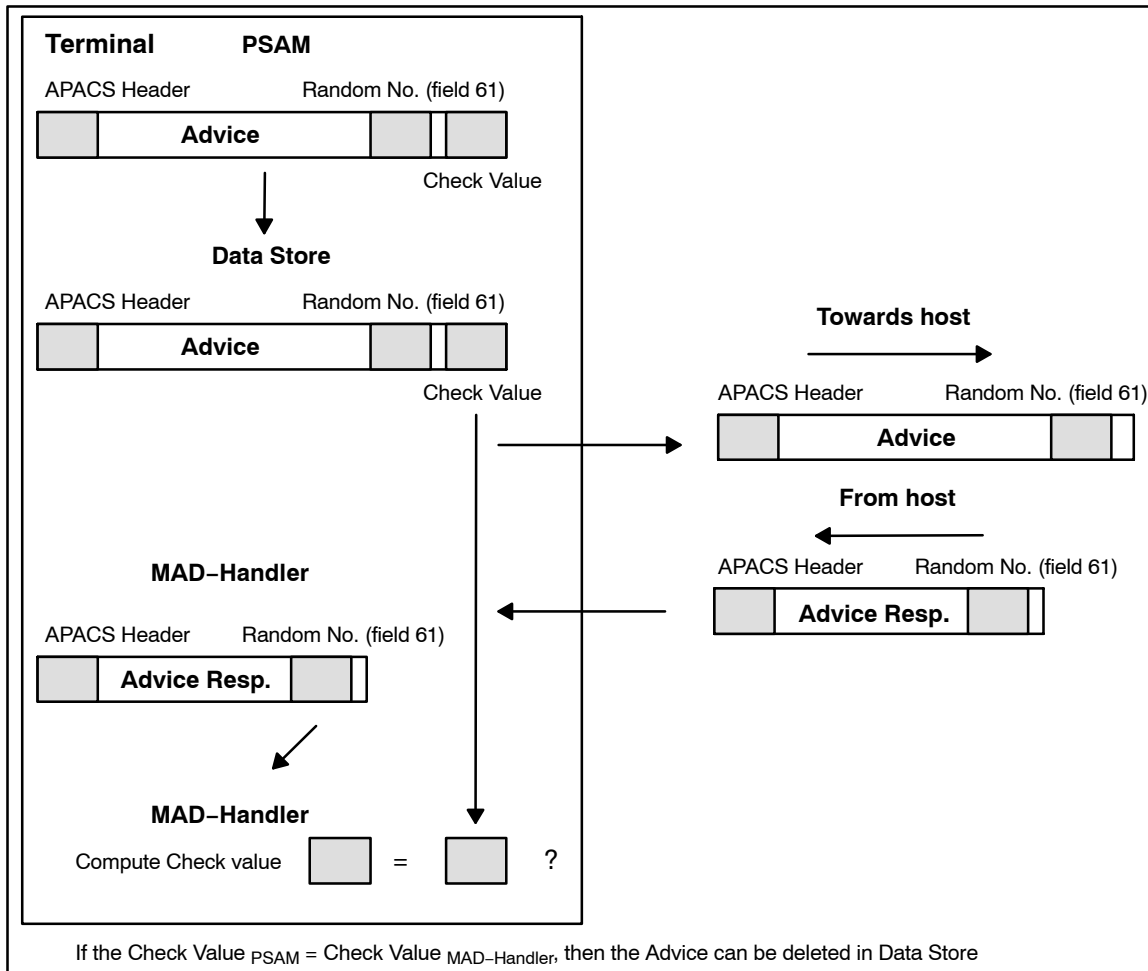


Figure 2-5.36 - Check Value Handling

2-5.15.5 Advice Window Size

Each time the terminal receives a response from the Terminal Operator host, the host may indicate an "Advice Window Size" in the APACS header.

Advice Window Size defines the maximum number of outstanding advices that the terminal may send before corresponding responses shall be awaited. Advice Window Size is relevant for the transfer of advices only but may be found in a variety of response messages. See table 2-13.9 Host Generated Data Objects in the APACS Header.

NOTE: The value of the Advice Window Size depends of the load at the host and may be in the range from 000 to 001.

The Advice Window Size is controlled by the Terminal Operator's host while the data element Terminal Advice Window Size is maintained by the terminal.

The format of the Advice Window Size is defined in section 2-13.7.9 page 2-13-15.

If the Terminal tries to have more outstanding advices than the Terminal Operator Host has indicated in the Advice Window Size the Communication Session may be terminated by the host.

- 2-5.15.5.1 A The MAD-Handler shall be able to control the number of outstanding advices i.e. advices sent but no corresponding response received yet.
- 2-5.15.5.2 A When a new Communication Session is initiated, the Terminal Advice Window Size shall be reset to 001.
- 2-5.15.5.3 A If the Advice Window Size given in the APACS header is 000, the MAD-Handler shall alter the Terminal Advice Window Size to a size of 000.
- 2-5.15.5.4 A If the Terminal Advice Window Size is 000 and the Advice Window Size given in the APACS header is 001, the MAD-Handler shall alter the Terminal Advice Window Size to a size of 001.
- 2-5.15.5.5 A When the outstanding advices reach the number in Terminal Advice Window Size, no further advices must be transmitted before the number of outstanding advices again are lesser than the number given in the Terminal Advice Window Size.
Figure 2-5.37 page 2-5-109 gives an example of Advice Window Size handling.
- 2-5.15.5.6 B A successful Advice Transfer shall be followed by a PSAM Update transaction as defined in section 2-5.13.3 page 2-5-93.

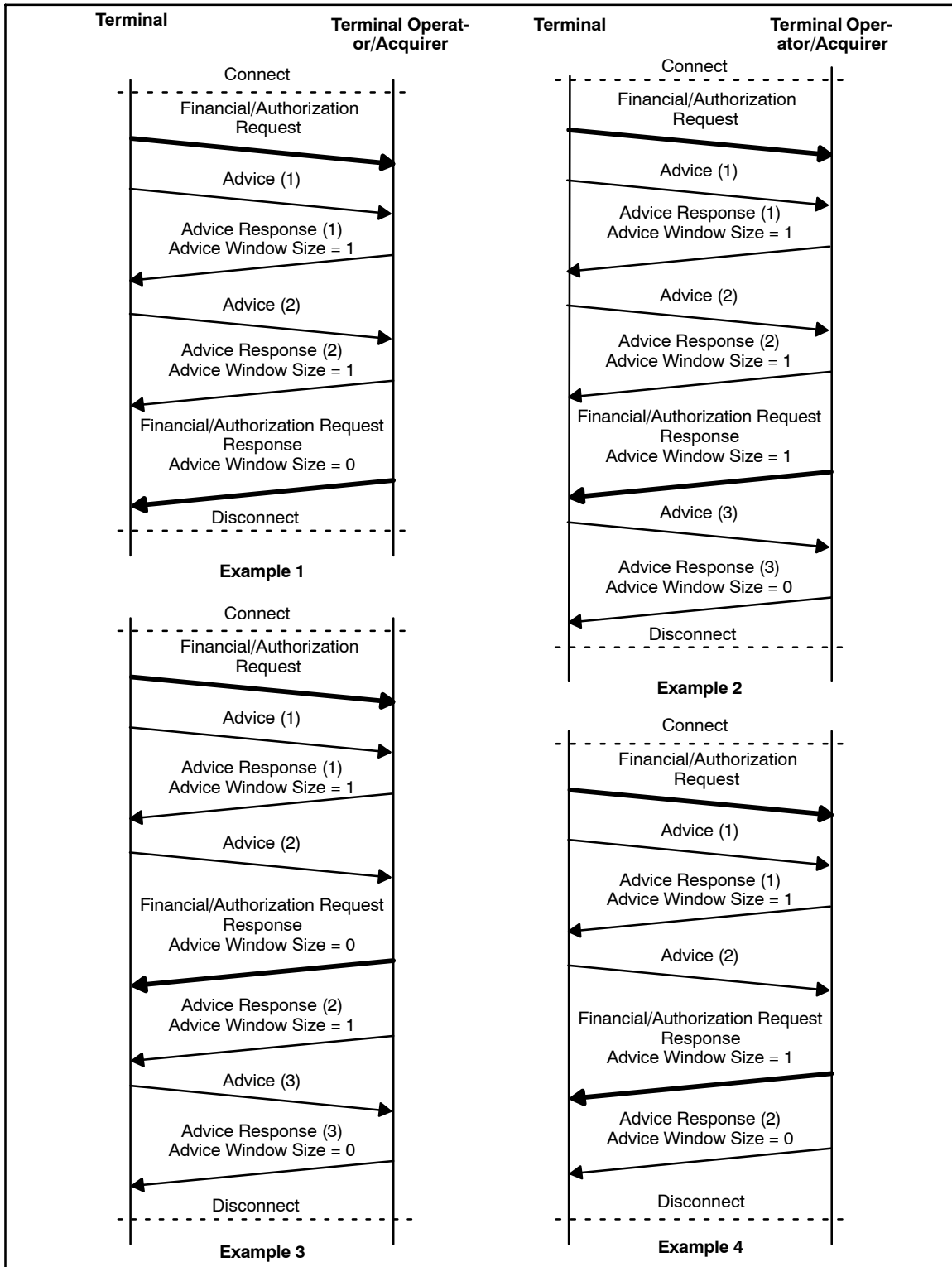


Figure 2-5.37 - Advice Window Size (Examples)

2-5.15.6 Counters and Batch Numbers

- 2-5.15.6.1 C When performing the Advice Transfer, counters maintained by the terminal/Merchant Application may optionally be reset.
- 2-5.15.6.2 C When performing the Advice Transfer, the Batch Number maintained by the terminal/Merchant Application may be adjusted.

An example of counter information to be updated during an Advice Transfer can be found in section 2-4.18 page 2-4-34, "Counters and Batch Numbers". The command sequence for an Advice Transfer is described in the figure 2-5.38.

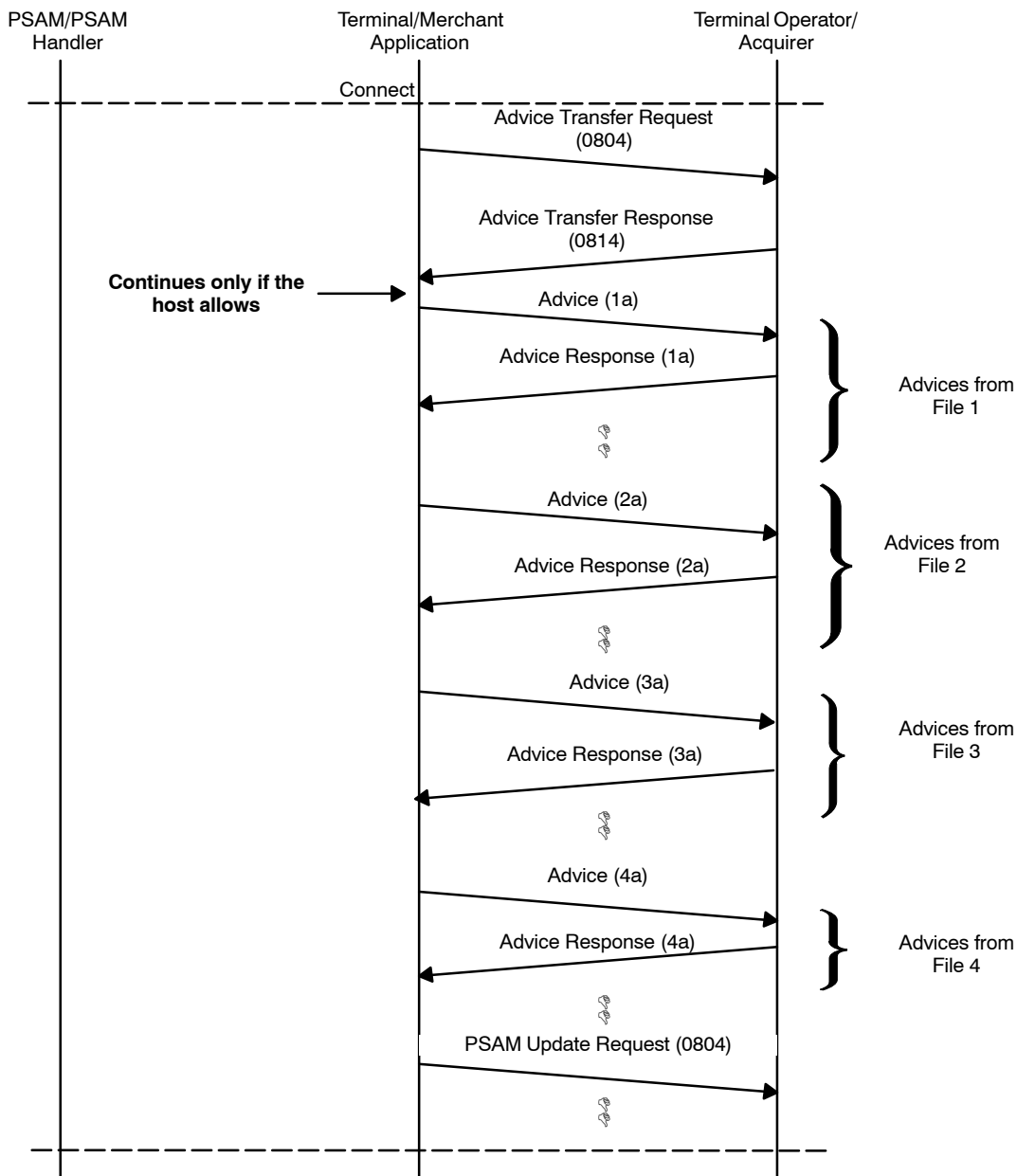


Figure 2-5.38 - Advice Transfer

Except for the Service Record that may be created after the mandatory PSAM Update, the Data Store does not contain any advices after a successfully completed Advice Transfer.

2-5.15.7 Exception condition - Accumulated Advices

If, for some reason, the terminal is unable to go online, the Merchant can choose to complete transactions offline using Temporary Offline Procedure, see section 1-9.10 page 1-9-5. This will result in an accumulation of advices in the terminal.

- 2-5.15.7.1 A Whenever it is possible to complete transactions online again, the terminal shall proceed with delivering advices as usual.

Other than the load distribution described in section 2-5.14.5 page 2-5.14.5, the terminal must not implement any form of load distribution of the delivery of advices as the load distribution is controlled by Nets Denmark A/S by using the Advice Window Size and thereby also the Terminal Advice Window Size.

However, the terminal may use one connection for sending requests and another for sending advices.

2-5.15.8 Exception Conditions, Failed Delivery of Advices

General

This specification defines that the Data Store in a Debit/Credit terminal shall include 4 files. The PSAM adds records to the 4 files according to this specification and the TAPA specification.

The terminal application controls the transfer of records from the Data Store to the host systems, and based on the individual responses from the host systems, the terminal application deletes the individual records from the Data Store.

If the terminal application does not receive a 'positive' response, i.e. the host rejects the record or the check value received does not match, the terminal application cannot delete the corresponding record from the Data Store and the records will remain in the Data Store 'forever'.

This section defines additional guidelines and requirements concerning the manual erasure of such 'defective records', and in general how to transfer advices from the Terminal Supplier's support system to Nets Denmark A/S.

The 4 debit/credit files defined in Data Store are in the following part of the present document called File 1 to File 4.

The Merchant Application Log (section 2-5.1.3 page 2-5-6) can be helpful if problems are detected in the Data Store.

The solution and guidelines stated in the present document are intended to make it possible to design and develop the necessary tools.

The fifth file (File 5)

The solution described below is based on the introduction of a fifth file in Data Store called File 5.

The same result may be obtain by the implementation of other techniques (e.g. by 'marking' records as defective without moving these records to another file), but the present document only describes the principles when using File 5.

- | | | |
|------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.15.8.1 | A | File 5 file shall be created by the terminal application. The PSAM only requests the creation of File 1 file to File 4 file. |
| 2-5.15.8.2 | A | File-5 shall be able to store records with a maximum length corresponding to the maximum value defined for File 1 to File 4 (plus an overhead for additional data if necessary). |

Conditions for moving advices to File 5

An advice may not be accepted by the host, i.e. the advice is rejected, or the terminal may not be able to accept the Random

- Number received (see section 2-5.15.4). Finally, the host systems may not reply due to e.g. security reasons.
- An advice is considered as not accepted if either:
- The Action Code is not in the range 8000 - 8005 (Accepted)
 - The Random Number is not acceptable
 - The advice has been sent, but no response has been received
- 2-5.15.8.3 B When transferring advices to the host systems, the terminal shall resend, if relevant, an advice two times in the communication session in progress before moving on to the next advice in line.
- 2-5.15.8.4 A Only when an advice have been resent in minimum 3 (three) different communication sessions without the conditions for deletion of the advice having been met, shall the terminal move the advice to File 5.
- 2-5.15.8.5 A The terminal must ensure that communication problems are not the reason the advice cannot be deleted from the Data Store.
- NOTE:** Requirement 2-5.15.8.5 can be ensured by e.g. performing an Advice Transfer. If no response to the Advice Transfer Request is received, it is most likely that there are communication problems and hence the advice is not to be moved to File 5.
- 2-5.15.8.6 A When a record is moved to File 5, the date and time for adding the record to File 5 shall be saved together with the original record data.
- When a 'defective advice' has been moved to File 5, the terminal may proceed with any ongoing processes, e.g. complete an Advice Transfer.
- 2-5.15.8.7 A When advices have been moved to File 5, a warning shall be issued to relevant parties, i.e. the Merchant for attended solutions and Back Office-systems for unattended solutions.
- 2-5.15.8.8 A The warning shall include, in the case of attended solutions, a guideline for handling the rejected advice(s).
- NOTE:** The guideline can be a reference to printed documentation e.g. an operating manual or similar.
- 2-5.15.8.9 C The warning to the Merchant may be issued both on the Merchant Display and be printed.
- 2-5.15.8.10 A The messages issued shall contain the following information on all advices stored in File 5:
- date and time for adding record to File 5,
 - STAN
 - Action Code (if any)
 - other information if relevant (e.g. no host response, wrong check value).

Operation of the terminal with advices stored in File 5

The terminal can continue normal operations, i.e. only warnings are issued, while having a number of advices stored in File

5. However, the number of files allowed in File 5 while continuing normal operations is limited.

2-5.15.8.11 A Whenever any advices are stored in File 5, performing an Advice Transfer shall include transfer of advices stored in File 5.

2-5.15.8.12 A When advices stored in File 5 are included, these advices shall be transferred as priority 5.

NOTE: The previous requirement for entering an 'error state' when files were transferred to file 5 has been removed.

Deleting records from File 5

2-5.15.8.13 A It shall only be possible to erase advices from File 5.

NOTE: It may be possible for an administrator at the Terminal Supplier to manually delete everything in the terminal Data Store. This must be a specially protected function only available to the Terminal Supplier.

2-5.15.8.14 A The erasure of advices from File 5 must be a specially protected function not readily available to the daily users of the terminal.

2-5.15.8.15 A The access to the function with which deletion of advices from File 5 is possible, shall be protected at least by a password unique to this function

2-5.15.8.16 B Access to the function shall only be possible by contacting the terminal supplier.

2-5.15.8.17 C A communication link between the Terminal Supplier's support system and the terminal may be established to control the erasure.

2-5.15.8.18 A A pre-approval of the chosen principle for the protection of the function for deletion of advices from File 5 shall be obtained from Nets Denmark A/S.

2-5.15.8.19 A Whenever the function is accessed, a warning shall be displayed or printed before final access is granted.

2-5.15.8.20 A The warning displayed and/or printed shall explain that the user is about to delete advices with potential economic impact on the business.

NOTE: The actual wording of the warning is out of scope of this specification.

2-5.15.8.21 A An Advice Transfer to the host systems covering all records stored in File 5 shall be attempted before the deletion of advices may commence.

2-5.15.8.22 A The information stored in a record in File 5 shall be logged before the concerned record may be deleted.

2-5.15.8.23 A The log shall as a minimum cover the following elements:

- the complete 'binary' data contents of the original record,

- information indicating the original file (File 1 to File 4),
 - date and time for adding record to File 5,
 - date and time for deleting record from File 5
 - why has the record been added to File 5 (e.g. no host response, wrong check value, Action Code).
- 2-5.15.8.24 C The log-information may be electronically transferred from the terminal to the Terminal Supplier's support system, before the concerned record is deleted from File 5.
- 2-5.15.8.25 B If the log-information is not transferred electronically to the Terminal Supplier's support system, the log-information shall be logged locally from the terminal, e.g. by printout using the receipt printer.
- 2-5.15.8.26 A If the log-information is logged on a non-electronic media, each byte of the 'complete binary data content of the original record' shall be printed as a 2-character hexadecimal value, and the log-information must include a check-value calculated on the 'complete binary data content of the original record'.
- The check-value makes it easier to validate the data entry, if the original record shall be re-established electronically by manually key-entering based on printed log-information. The algorithm used to calculate the check-value is outside the scope of this specification.
- 2-5.15.8.27 C The log-information covering records deleted from File 5 may be transferred to the Terminal Supplier for further investigation and registration.
- 2-5.15.8.28 C The general terminal-log (or journal) covering all transactions in the relevant settlement period may also be transferred to the Terminal Supplier.
- Based on the log-information covering records deleted from File 5, combined with the general log from the terminal for the concerned settlement period, it may be possible to manually investigate what the original record contained.

Transfer of Advices from support system

If the result of the investigation makes it possible to correct the record and re-establish the original record, it may be possible to re-send the corrected record from the Terminal Supplier's support system to the host system, and in this way minimize the risk for lost records.

The transfer of records saved from the Data Store can be performed using either a terminal especially enabled for import of advices or a system capable of performing the data transfer as defined for the terminal.

Such a terminal or system does not necessitate the usage of a PSAM as the records contains all necessary information for handling in the host system.

The advices are transferred using the same TCP/IP setup as for the normal production terminals.

- 2-5.15.8.29 C The transfer of records may be performed according to the procedures defined for Advice Transfer or according to the Send Advices procedure, i.e. omitting the request message.

2-5.16 Exception Handling

2-5.16.1 General Rules

There are a variety of exception conditions that can occur during the dialog between the terminal & PSAM, card & terminal and terminal & host. This section defines a set of functions that must be provided by the terminal in order to allow various types of error recovery. See also ref. 27: "TAPA; Application Architecture Specification", section 4.3.

Actions to be taken upon ASW1-ASW2

Figure 2-5.39 gives a clarification of which action to be taken when unsuccessful ASW1-ASW2 are returned. This figure is based on the requirements stated in section 2-14.10.1 page 2-14-131.

NOTE: Figure 2-5.39 page 2-5-116 only covers ASW1-ASW2 values which require special action.

- 2-5.16.1.1 A If the PSAM responds with an ASW1-ASW2 indicating an unsuccessful operation to a command or the MAD-Handler encounters an error, the MAD-Handler shall send a *Complete Payment* command to the PSAM in order to make the PSAM "clean-up" all processes related to this ID_{THREAD} and return to idle. At the same time, a *Transaction Completed* command shall be send to the Merchant Application indicating that the transaction failed.

The PSAM can be considered "ready" (and the ID_{THREAD} released) when a successful response to the *Complete Payment* command has been received.

If the PSAM responds with an ASW1-ASW2 indicating an unsuccessful operation to a command, the field "Transaction Status" in the *Complete Payment* command will be ignored by the PSAM.

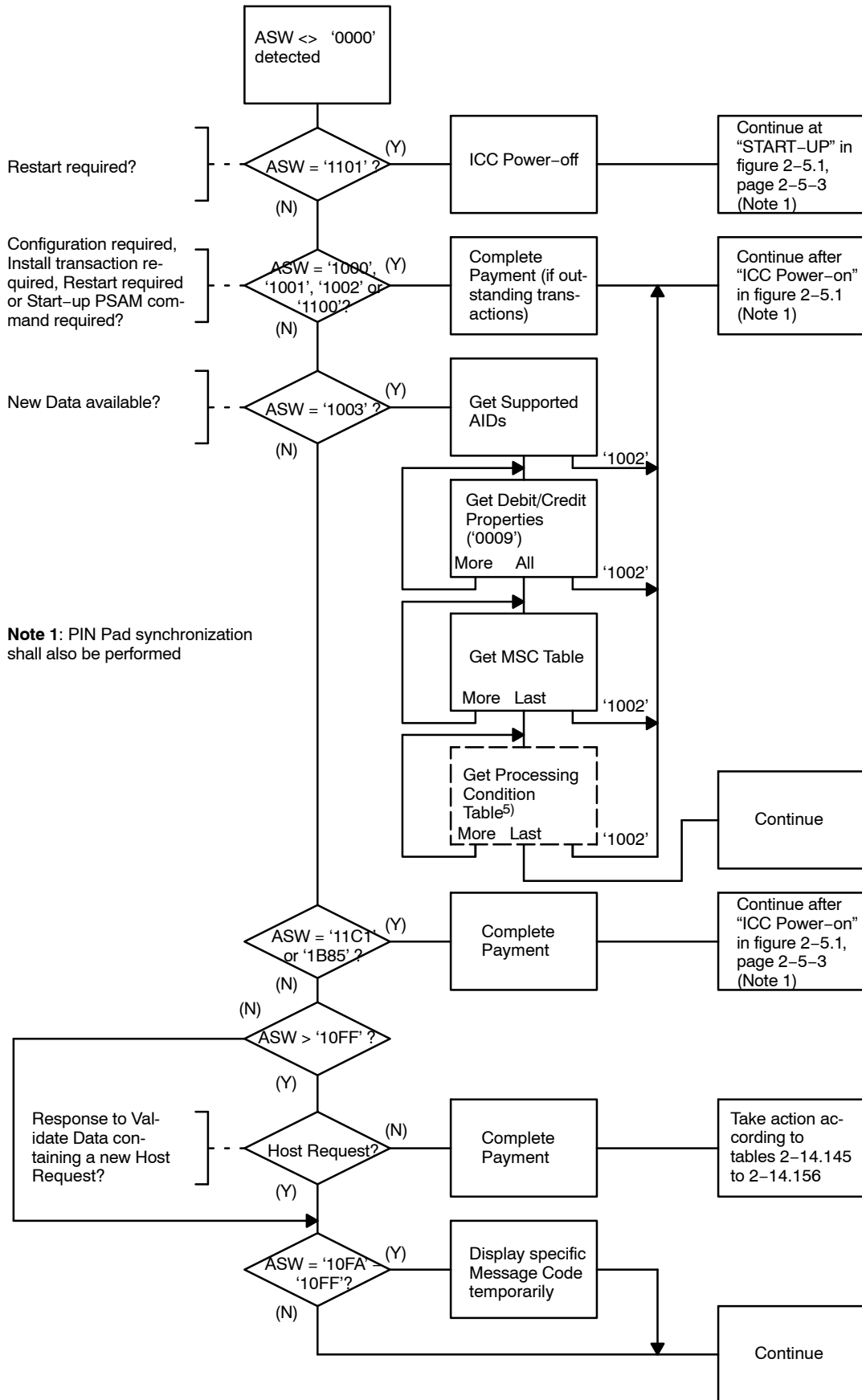


Figure 2-5.39 - Handling of ASWs which Require Special Action

Three main categories of errors exists:

Errors occurring before the selection of the terminal application

- 2-5.16.1.2 A The MAD-Handler shall indicate the type of error in one of the error counters specified in section 2-13.6 page 2-13-12 Communication Statistics and Error Counters.

The status of these counters is given in the field "Statistics" in the *Initiate Payment* command and is conveyed to the host in either the APACS header or field 46 of a message.

Errors occurring after the debit/credit application has been selected (and the PAN is recognized) and before an online session has been established.

The PSAM will always create an Authorization Advice. The response to either *Initiate Payment* or *Payment* command will in this case indicate an unsuccessful operation.

Errors occurring after an online connection has been established.

Either the host, card or PSAM may decide to decline the transaction. No Authorization Advice is be created, but in the case where the PSAM/card declines an approved transaction from the host, the PSAM will create a Reversal. If the transaction is chip-based and a rejection is received from the host, the PSAM will generate a reversal.

If an error occurs during an offline transaction, the PSAM will create an Authorization Advice.

No host response

If the terminal sends a request but no host response is received, the terminal can resend the request using the rules for repeats.

If the terminal sends an advice but no host response is received, the rules defined in section 2-5.15.8 "Exception conditions, Failed Delivery of Advices" applies.

2-5.16.2 Categories

Exception handling falls broadly into the following categories:

- Terminal related errors
- PSAM related errors
- Transmission errors
- Host declined transactions
- PSAM declined online transactions
- PSAM declined offline transactions
- Card declined transactions
- Cardholder initiated actions

2-5.16.3 Terminal Related Errors

Installation/Start-up

- 2-5.16.3.1 A Whenever the terminal has been updated (hardware has been replaced as well as a new software version has been loaded), the terminal shall initiate a total configuration of the terminal by issuing the following commands:

- *Start-up PSAM*
- *Exchange Debit/Credit Static Information*
- *Get Supported AIDs*
- *Get Debit/Credit Properties*
- *Get MSC Table*
- *Get Debit/Credit File Characteristics*
- *Configure PSAM Application*
- *Synchronize PSAM/PIN Pad*

NOTE: Prior to updating the terminal, the content of the Data Store files must be forwarded to the Terminal Operator/acquirer.

NOTE: Replacement of e.g. the Data Store will also require a total configuration.

Card Related Transactions

- | | | |
|------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.16.3.2 | A | In case of erroneous reading of an EMV card, the exception handling shall follow rules defined in ref. 20: "EMV ICC Specification". |
| 2-5.16.3.3 | A | Exception handling related to online Authorizations and Advices in case of an EMV card shall follow the requirements given in ref. 20: "EMV ICC Specification". |
| 2-5.16.3.4 | A | In case of erroneous reading of a MSC, the cardholder shall be prompted to swipe/insert the card again by displaying the Message Codes 'E3'/'13' ("Error reading card"/"Try again") on the Cardholder Display. |

Merchant Application

- | | | |
|------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.16.3.5 | A | If a communication error occurs between the CAD and the Merchant Application, the terminal shall increment the data element "Number of communication errors between CAD and Merchant Application". |
|------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Terminal Shut-down

- | | | |
|------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.16.3.6 | A | <p>During exception situations, it may be necessary to shutdown the terminal (either to attempt a restart or to permit human intervention). Prior to shutting down the terminal, the MAD-Handler shall, if possible:</p> <ul style="list-style-type: none"> • Attempt to complete all in-progress transactions (by sending a <i>Complete Payment</i> command for each current ID_{THREAD}). • Attempt to shutdown the PSAM application "gracefully" by sending the <i>PSAM Shutdown</i> command. |
|------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2-5.16.4 PSAM Related Errors

Installation/Start-up

- | | | |
|------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.16.4.1 | A | If initialization of the debit/credit application fails, the MAD-Handler shall re-issue the commands necessary to make the terminal ready for transactions, starting with the <i>Start-up PSAM</i> command. |
|------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

PSAM Updates

- 2-5.16.4.2 A If the following ASW1-ASW2 values are returned, the terminal shall re-send the PSAM Update(s):
- PSAM busy - Try later ('1151')
 - PSAM busy - Active threads ('115A')

- 2-5.16.4.3 A For all other values of the ASW1-ASW2 returned, the terminal shall discard/delete the PSAM Update(s).

NOTE: Updates not accepted by the PSAM will be re-sent from the host when requested by the terminal.

Firmware Checksum Error

The PSAM will regularly check the integrity of the firmware. This will be initiated during *Start-up* and during the *Initiate Payment* command at least once a day.

In case of any alteration of the firmware, different actions can be initiated from the PSAM. The severeness of the actions goes from returning a soft ASW1-ASW2 (value < '1100') to making the PSAM inoperative in an irreversible process.

If the PSAM has been made inoperative, the PSAM will respond with SW1-SW2 = '6E 00' on all commands.

- 2-5.16.4.4 A The terminal shall be able to handle a Service Record added to the Data Store by the PSAM when the *Complete Payment* command is issued.

NOTE: Adding this Service Record may in worst case introduce up to three different messages to be stored in the Data Store during a transaction, e.g. a Financial advice, Reversal Advice (in case of Data Store problems) and a Service Record.

- 2-5.16.4.5 C If the PSAM has been made inoperative, the terminal should inform the merchant of this event.

NOTE: Even though the PSAM is inoperative, Advice Transfer shall be possible if the Data Store contains any advices, see requirement 2-5.15.2.3.

2-5.16.5 Host Declined Transactions (Requests)

NOTE: For handling of host declined advices, see section 2-5.15 page 2-5-101.

Generation of a new Host Request

The PSAM may generate a new host request due to the data received in the response to the host request.

As example, an online PIN validation has failed, and the PSAM/terminal offers the cardholder to key in the PIN without entering the card again (PIN retry). The transaction flow is not terminated at this moment and the other transaction data are kept intact, e.g. amount. See the transaction flow depicted in figure 2-5.40 page 2-5-121. The ASW1-ASW2 returned in the response to *Validate Data 2* command is '10FF' ("Incorrect PIN") when a new try is performed.

- 2-5.16.5.1 A Whenever the response to the *Validate Data 2* command contains a length field $LEN_{STAN+HREQ}$ different from '0000', the terminal shall send the entire host request.

The response to the *Validate Data 2* command contains a new host request only, if the use of at least Service Pack No. 1 has been requested and accepted.

The Systems Trace Audit Number, STAN, and the new host request is contained in the response to the *Validate Data 2* command, see section 2-14.6.3 page 2-14-59.

In case of PIN retry, the PSAM will request the cardholder to confirm the amount and enter the PIN again during the *Validate Data* processing.

When a new host request is generated, the PSAM assigns a new value of the STAN. This new value shall be used on e.g. receipts and total reports.

- 2-5.16.5.2 A If a new host request is generated, the terminal shall initiate a renewed *Validate Data 2* command when the response to the host request is received according to the example given in figure 2-5.40 page 2-5-121.

The handling of a new host request has priority to the Application Status Words (ASW1-ASW2).

In case of PIN retry, several different host requests may be expected each containing an unique STAN.

In case of EMV transactions, the first response to the host request may contain issuer scripts changing the environment in which the transaction is performed, e.g. a *Card Blocked* command. Hence there can be no online PIN retry during EMV transactions.

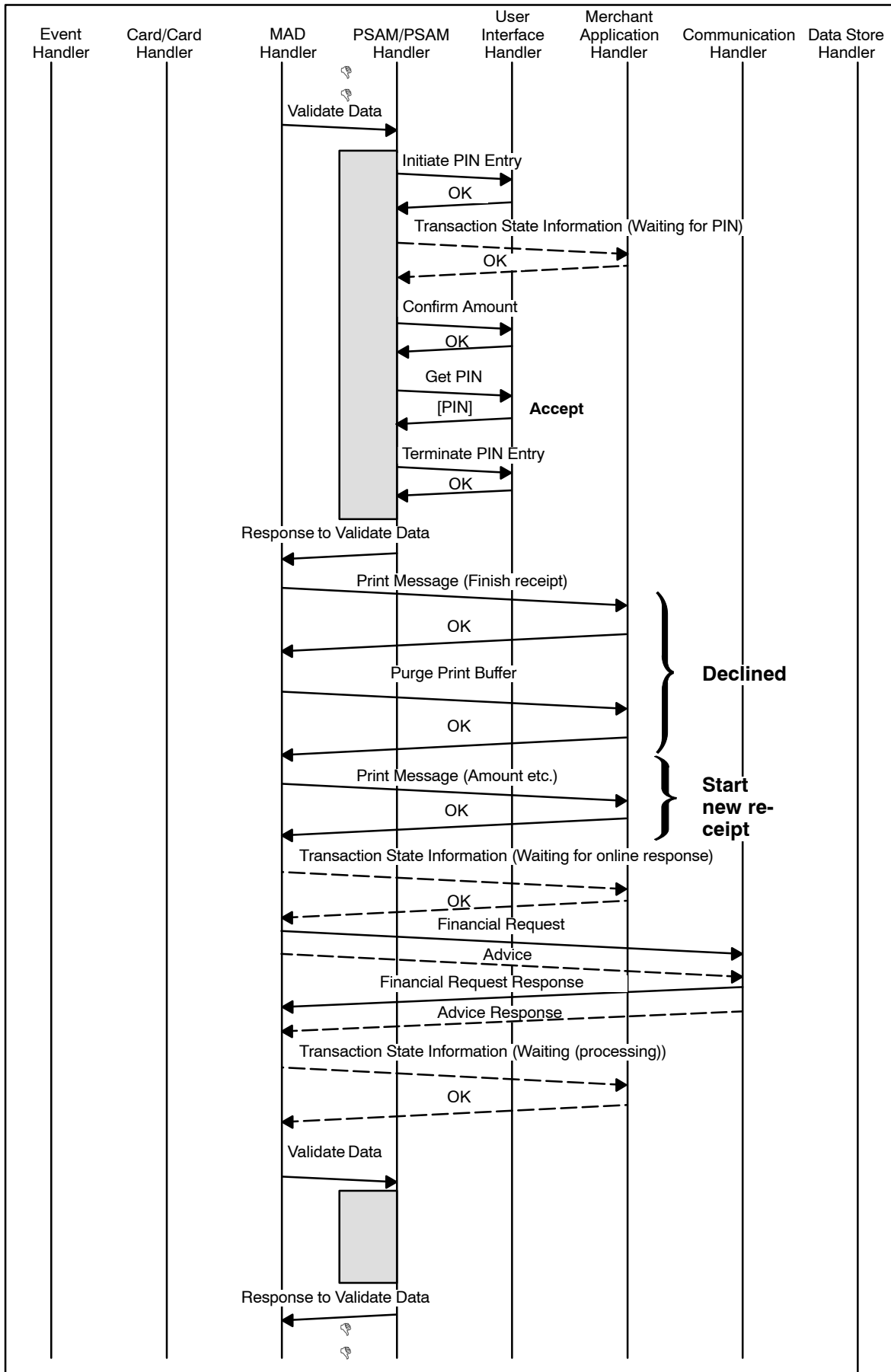


Figure 2-5.40 - PIN Retry Flow

2-5.16.6 Application Status Words

The action to be taken by the terminal in case of transactions where the PSAM is involved, is indicated in the Application Status Words (ASW1-ASW2). The action to be taken and the relevant Message Code for the Merchant Display can be found in section 2-14.10.1 page 2-14-131, table 2-14.142 page 2-14-133 to table 2-14.156 page 2-14-155.

2-5.16.7 PSAM Declined Online Transactions

The PSAM may overrule a successful transaction result indicated in the Action Code by the host, e.g. if the MAC validation failed. The PSAM will then create a Reversal Advice which will be saved in the Data Store when the *Complete Payment* command is sent to the PSAM.

2-5.16.8 PSAM Declined Offline Transactions

The PSAM may overrule a successful transaction result indicated by the card, e.g. if the card is found on the Stop List. The PSAM will then create a Reversal Advice which will be saved in the Data Store when the *Complete Payment* command is sent to the PSAM.

2-5.16.9 Card Declined Transactions

Card declined transactions will be dealt with by the PSAM. SW1 SW2 originating from the card will in some cases be forwarded transparently from the card to the MAD-Handler by the PSAM.

From the terminal's point of view, the exception handling is identical to handling of the PSAM related errors.

2-5.16.10 Cardholder Initiated Actions

Cancel button

If the Cancel button is activated while the PSAM processes the transaction, the cancellation may be effective during one of the following "waiting points":

- *Get Amount* command, awaiting amount entry
- *Get PIN* command, awaiting PIN entry
- *Confirm Amount* command, awaiting amount acceptance (and PIN if combined mode is used)

When the cancellation is initiated during the *Get Amount* command and the command is addressed to the Merchant Application Handler, the Merchant Application Handler must be informed by the User Interface. This information may e.g. be transferred using the Event Handler.

- | | | |
|-------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-5.16.10.1 | A | The Cancel button shall be active until the cardholder has confirmed the amount (and for PIN related transactions, both amount and PIN). |
| 2-5.16.10.2 | A | If the cardholder press the Cancel button during the transaction initialization, the terminal shall return to idle and terminate all processes related to this transaction by issuing <i>Complete Payment</i> command(s) to the PSAM. |

- 2-5.16.10.3 A If the cancellation is initiated during the *Get Amount* command (baseline), the response to this command shall contain the Response Code 'FFF2' (time-out) independent of Service Packs
- NOTE:** No dedicated Response Code has been defined to indicate "Transaction interrupted", but since the reaction shall be identical for cancel- and time-out situations, the Response Code indicating "Time-out" shall be used.
- NOTE:** See table 2-8.2 on page 2-8-7 for further details concerning the behavior of the different variants of the *Get Amount* command.
- 2-5.16.10.4 A If any subsequent *Get Amount* command is issued after the cancellation is initiated as defined in requirement 2-5.16.10.3, the response shall contain the Response Code 'FFF2' as well.
- NOTE:** Subsequent *Get Amount* commands may occur in the situations described in section 2-8.4.2. Although this section refers to the *Get Amount 2* command, the principle is valid for the *Get Amount* command too.
- 2-5.16.10.5 A If the cancellation is initiated during the *Get PIN* command, the response to this command shall contain the Response Code 'FF86' indicating "PIN not available".
- NOTE:** When the combined mode for PIN entry and amount confirmation is used, the *Get PIN* command will not initiate a "waiting point" since the PIN code is ready to be included in the response. In this situation the amount (and PIN) has already been confirmed, and the activation of the Cancel button shall therefore be neglected.
- 2-5.16.10.6 A If the cancellation is initiated during the *Confirm Amount* command, the response to this command shall contain the Amount Confirm Indicator '02' indicating "Cancelled by user".

2-5.16.11 Communication Statistics and Error Counters

See description in section 2-13.6 page 2-13-12 and 2-13.9.11 page 2-13-87 respectively.

2-5.16.12 Authorization Advice

A Reversal Advice or Authorization Advice will be created by the PSAM whenever an error has been encountered by the PSAM. It will be an Reversal Advice if the transaction has been sent online. Authorization Advices are created in order to inform the host of the particular error related to a certain card.

2-5.16.13 Message Codes

- 2-5.16.13.1 A In case of a rejected transaction, the display/print Message Code shall conform to the guidelines given in section 2-14.10.1 page 2-14-131 where the appropriate Message Code is given for each Application Status Word (ASW1-ASW2). The text and Message Codes are applicable for the Merchant Display.

2-5.16.14 Action Codes

The Action Codes conveyed in field 39 of the APACS response message shall in general *not* be interpreted by the terminal except for position 2 which may indicate to the terminal how to control the communication line. The Application Status Words (ASW1-ASW2) from the PSAM will reflect the action to be taken by the terminal.

The Action Code conveyed in field 39 of the host response or in the response to *Validate Data 2* command shall be used when printing the receipt. See section 1-12 page 1-12-1.

NOTE: When performing administrative transactions, requirement 2-5.13.1.1 page 2-5-91 applies!

Action Codes with 8 in position 1 (reserved for national use) will appear when the PSAM is not involved in the communication between terminal and host, e.g. Advice Transfer. Action Codes starting with 8 in position 1 are applicable for the message types 0136, 0236, 0436, 0634 and 0814 (response to: Advice Transfer, PSAM Update and Clock Synchronization). See also section 2-13 page 2-13-1.

These Action Codes indicate the status of e.g. each Advice delivered to the host and the terminal shall act according to the Action Code received. The Action Codes may also be used for reporting purposes. The transfer of e.g. Advices may take place as a "background job" while the terminal is performing an online request.

If the transfer takes place as a "background job", the result of the transfer may be logged only (and not displayed) since any message displayed may confuse the Merchant who is engaged servicing a cardholder.

If the result of the actual communication sequence has significance for the merchant at the time when the result is received, a message text shall be displayed.

Action Codes defined for national use can be found in table 2-5.6 page 2-5-125.

Table 2-5.6 - Action Codes (National Use)

Action Code	Description	Message Code	Text ²⁾ (Merchant Display)
8000	Accepted/Successful	'03' ¹⁾	"Approved"
8001	Accepted, unspecified mismatch in data	'03' ¹⁾	"Approved"
8002	Accepted, format error (e.g. MAC error)	'03' ¹⁾	"Approved"
8003	Accepted, card data mismatch	'03' ¹⁾	"Approved"
8004	Accepted, merchant data mismatch	'03' ¹⁾	"Approved"
8005	Accepted, PSAM ID mismatch	'03' ¹⁾	"Approved"
8020	Rejected	'07' ¹⁾	"Declined"
8421	Rejected, try again later	'13' ¹⁾	"Try Again"
8022	Rejected, format error (e.g. MAC error)	'07' ¹⁾	"Declined"
8023	Rejected, card data mismatch	'07' ¹⁾	"Declined"
8024	Rejected, merchant data mismatch	'07' ¹⁾	"Declined"
8025	Rejected, PSAM ID mismatch	'07' ¹⁾	"Declined"

Legend:

¹⁾ May not be displayed (transfer may run in the "background").

²⁾ The table show the generic texts in English, see section 1–15. for regional texts.

2-5.16.15 Merchant Initiated Actions

Merchant Cancel Button

A Merchant Cancel button may be implemented as part of the Merchant Application.

This button may be seen as a parallel to the Cancel button required as part of the User Interface.

By activating the Merchant Cancel button while the PSAM processes the transaction, the Merchant may be able to interrupt a transaction in progress.

Similar to activation of the Cancel button on the User interface, the Merchant Cancel button may initiate a cancellation during one of the following "waiting points":

- *Get Amount* command, awaiting amount entry
- *Get PIN* command, awaiting PIN entry
- *Confirm Amount* command, awaiting amount acceptance (and PIN if combined mode is used)

The cancellation may also be initiated during other command/response sequences.

If the cancellation is initiated during the *Get Amount* command and this command was addressed to the User interface Handler, the User Interface Handler must be informed by the Merchant Application Handler. This information may e.g. be transferred using the Event Handler.

Similar when cancellation is initiated during *Get PIN* or *Confirm Amount* commands, the User Interface shall be informed by the Merchant Application.

- 2-5.16.15.1 C The cancellation shall be indicated in the respective responses as defined when activating the Cancel button on the User Interface, see section 2-5.16.10 page 2-5-122.

2-5.16.16 Time-outs

The following commands may include a time-out value:

- *Get Amount* command, awaiting amount entry
- *Get PIN* command, awaiting PIN entry
- *Confirm Amount* command, awaiting amount acceptance (and PIN if combined mode is used)

Other discretionary commands may include a time-out value.

- 2-5.16.16.1 A If a time-out value expires while awaiting either amount entry, PIN entry or amount confirmation, the terminal shall end the transaction in progress.

NOTE: This may be seen as a parallel to activating the Cancel button on the User Interface.

- 2-5.16.16.2 C If the commands do not include a time-out value, the destination handler (Merchant Application or User Interface) may include a default time-out value used instead.

NOTE: A value between 60 and 180 seconds may be reasonable as default time-out value.

- 2-5.16.16.3 A If the time-out value expires during the *Get Amount* command, the response to this command shall contain the Response Code 'FFF2' (time-out).

- 2-5.16.16.4 A If the time-out value expires during the *Get PIN* command, the response to this command shall contain the Response Code 'FF86' indicating "PIN not available".

- 2-5.16.16.5 A If the time-out value expires during the *Confirm Amount* command, the response to this command shall contain the Amount Confirm Indicator '01' indicating "Not confirmed".

2-6 Design Requirements

2-6.1 General Considerations

2-6.1.1 Environmental Requirements

The terminal will be required to work in different environments according to the type of merchant and installation. Adequate precautions need to be taken to ensure that misoperation does not occur. These precautions should cover:

- Climatic environments:
- Mechanical environments:
- Electrical environments:
- Auditory environment:

The terminals are classified into 3 categories according to their implementation:

Category A: Terminals used in sheltered and heated rooms

Category B: Terminals used in rooms and shelter that are not heated

Category C: Terminals used outdoors (*outside*) without shelter.

- | | | |
|-----------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-6.1.1.1 | A | The terminal shall be able to operate in the intended environment. |
| 2-6.1.1.2 | A | The terminal shall be designed for unattended intermittent or continuous operation. |
| 2-6.1.1.3 | A | The Terminal Supplier shall ensure that the terminal complies with regulations specified by the authorities for the environment in which the terminal is to be installed. |
| 2-6.1.1.4 | A | The Terminal Supplier shall specify the environment for which the terminal is suitable to operate. |

2-6.1.2 Documentation

- | | | |
|-----------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-6.1.2.1 | B | The terminal shall be supplied with an installation guide. |
| 2-6.1.2.2 | B | The installation guide shall be in English and the merchant's local language. |
| 2-6.1.2.3 | B | The terminal shall be supplied with a detailed user manual for the merchant, i.e. detailed written information about the use of the terminal, e.g. daily use, administrative procedures and instructions for correcting any malfunction of the terminal. |
| 2-6.1.2.4 | B | The manual shall also contain relevant technical information, including guidelines for PSAM replacement. |
| 2-6.1.2.5 | C | The user manual may be in English and in the merchant's local language. |

2-6.1.3 Marking

Terminal and Terminal Supplier Information

- 2-6.1.3.1 B Each terminal shall be marked with the name of the Terminal Supplier.
- 2-6.1.3.2 B Each terminal shall be marked with a type number.
- 2-6.1.3.3 A Each terminal shall be marked with a unique serial number.

NOTE: The name of the manufacturer, the type number and the unique serial number may not necessarily be visible to the cardholder.

If it does not appear on the display a warning saying "Beskyt din PIN-kode" (protect your PIN-code), a permanent label shall be mounted in the vicinity of the PIN Entry Device. See requirement 2-7.2.2.5 page 2-7-3.

User Guidance

- 2-6.1.3.4 A User guidance shall be in the merchants local language . User guidance can be shown either on the Cardholder Display, or as a combination of fixed text on the terminal and messages on the Cardholder Display.
- 2-6.1.3.5 B User guidance shall also be available in English.
- 2-6.1.3.6 C User guidance in other languages is allowed, if guidance in the merchants local language and English is available as well.
- 2-6.1.3.7 C User guidance in pictograms, drawings or pictures may be implemented. See figure 2-6.1 for examples.
- 2-6.1.3.8 C The character type of text is recommended to be Helvetica or Modern.
- 2-6.1.3.9 B Terminals with a swipe-reader for magnetic stripe cards shall be equipped with a pictogram showing the cardholder how to swipe the card in the MSCR.
- 2-6.1.3.10 A Terminals with a motorized Card Reader shall be equipped with a pictogram showing the cardholder how to insert the card into the motorized Card Reader. See figure 2-6.1 for examples of pictograms.
- 2-6.1.3.11 A Terminals shall be equipped with a pictogram showing the cardholder how to insert the ICC into the ICCR. See figure 2-6.1 for examples of pictograms.

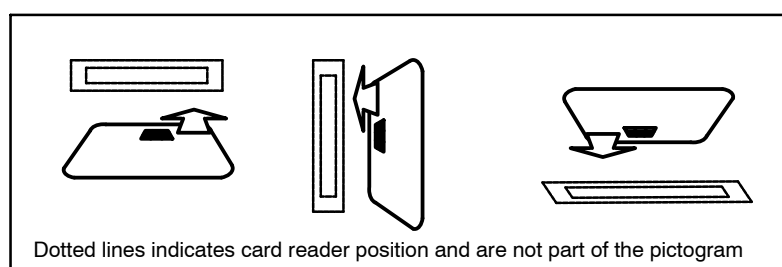


Figure 2-6.1 - Pictograms (Examples)

PIN Pad

- 2-6.1.3.12 B The PIN Pad shall be clearly marked with the PIN Pad ID loaded into the PIN Pad.

NOTE: The PIN Pad ID may for example be engraved or printed directly on the PIN Pad. Another example is to engrave or print the PIN Pad ID on a small piece of metal which is then welded, glued, laminated or by similar method integrated with the PIN Pad.

2-6.1.4 Servicing the Terminal

- 2-6.1.4.1 B The terminal shall be supplied with written instructions for correcting any foreseen malfunction of the terminal.

NOTE: Instructions can be a detailed error handling document and/or a phone number to a service technician.

2-6.2 Mechanical Design

2-6.2.1 General Requirements

- 2-6.2.1.1 A The terminal design of the Secure Device shall be in accordance with the requirements defined by the Payment Card Industry (PCI), see ref. 36: "POS PIN Entry Device Security Requirements Manual".

NOTE: If the ICCR or the display is not part of the Secure Device, it may introduce limitations in Cardholder Verification Methods supported and thus reduce the cards accepted. Furthermore, limitations concerning key entry may be introduced.

- 2-6.2.1.2 A Any activation of a hardware function or change in the terminal status shall cause an immediate reaction or response in the user interface.

- 2-6.2.1.3 A A 24 hour real time clock with calendar shall be part of core functions in the terminal. It shall include:
- Automatic correction for the number of days per month and leap years,
 - accuracy: ± 3 seconds per day and
 - battery back-up for minimum 30 days.

2-6.2.2 Combined Card Reader

- 2-6.2.2.1 B A UPT terminal shall have a combined card reader if magnetic stripe cards are supported.
- 2-6.2.2.2 C A POS terminal may have a combined card reader.

- 2-6.2.2.3 A A terminal with a motorized or locking combined card reader shall be equipped with an Eject button. The card shall be released when the Eject button is activated.
- 2-6.2.2.4 B The Eject Button shall be red, if implemented as a dedicated button.

2-6.2.3 Integrated Circuit Card Reader

- 2-6.2.3.1 A The terminal shall have a valid EMV Level 1 type approval.
- 2-6.2.3.2 A If the ICCR is not a motorized card reader, the card inserted shall be accessible for the user.
- 2-6.2.3.3 C The ICCR may contain a mechanism which is able to lock the inserted card during a payment sequence.
- 2-6.2.3.4 A If the ICCR contains a mechanism which is able to lock the card, the card shall be released if an error occurs, e.g. a power failure.
- 2-6.2.3.5 A Physical removal of the inserted card at any time shall not leave the terminal in an invalid or unknown state.
- 2-6.2.3.6 A The inserted card shall be inserted with the short side first.
- 2-6.2.3.7 B The short side nearest the contacts shall be inserted first.
- 2-6.2.3.8 B The contacts of the card shall face the cardholder, when the card is inserted using the right hand.

2-6.2.4 Magnetic Stripe Card Reader

- 2-6.2.4.1 B The MSCR shall have a service life comparable to the service life of the terminal which it is intended.
- 2-6.2.4.2 A The MSCR shall not damage any MSC swiped/inserted.
- 2-6.2.4.3 C A 'shutter' may be installed to protect the MSCR against insertion of irrelevant material.
- 2-6.2.4.4 B If the MSCR is a separate swipe-reader, there shall be no physical stop in either the beginning or end of the swipe slot.
NOTE: Unless it is a combined swipe and park reader.
- 2-6.2.4.5 B A separate MSCR shall be placed either in the top or in the right hand side of the cardholder operated part of the POS terminal
- 2-6.2.4.6 B It shall be possible to operate the MSCR with either hand.
- 2-6.2.4.7 B If the MSCR is a separate swipe-reader, the MSCR shall be able to read the MSC when swiped in either direction.

2-6.2.5 Visual Indicators

- 2-6.2.5.1 A The Cardholder Display shall, as an absolute minimum, be able to display two lines of text simultaneously.

- 2-6.2.5.2 B The Cardholder Display shall be able to display four lines of text simultaneously.
- 2-6.2.5.3 C The Cardholder Display may be able to display more than four lines of text simultaneously.
- 2-6.2.5.4 B Each line of text on the Cardholder Display shall be able to contain 20 characters simultaneously.
- 2-6.2.5.5 C Each line of text on the Cardholder Display may contain more than 20 characters.
- 2-6.2.5.6 A The Cardholder Display shall be alphanumeric.
Display messages defined in this specification, or otherwise desired by the Terminal Supplier, may exceed 4 □ 20 characters.
- 2-6.2.5.7 B Messages exceeding the capability of the Cardholder Display shall be edited in co-operation with PBS.
- 2-6.2.5.8 A The Cardholder Display shall be able to display all the intended display messages for the intended region.
NOTE: The messages in English and Danish can be found in table 1-11.2 and for other regions in the different sections of chapter 1-15.
- 2-6.2.5.9 B The character height of the Cardholder Display shall be at least 5.5 mm.
- 2-6.2.5.10 B LCD Cardholder Displays with a character height less than 6.5 mm shall be back-lighted (when in use).
- 2-6.2.5.11 B The Cardholder Display shall be readable in a viewing angle of at least $\pm 30^\circ$ from perpendicular to the surface. See figure 2-6.2.

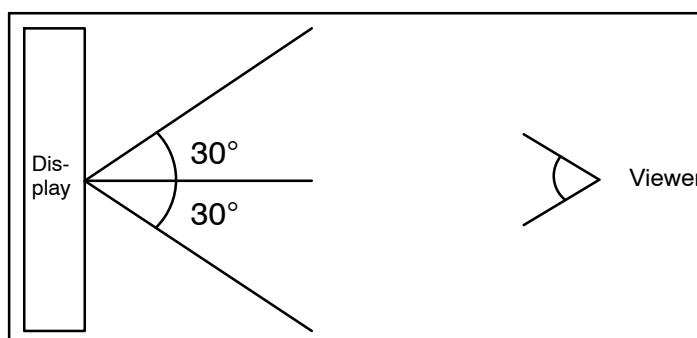


Figure 2-6.2 - Viewing angle

- 2-6.2.5.12 A Additional information displayed during the transaction shall not interfere with the readability. The area used for the dialogue with the cardholder shall be fixed and the text shall form a sharp contrast to background and the background shall be of uniform colour.
- 2-6.2.5.13 A The Cardholder Display shall be easily readable under the lighting conditions encountered in the intended environments.

2-6.2.6 Audio Indicator

The functional requirements can be found in section 2-4.8.2 page 2-4-14.

- 2-6.2.6.1 B The terminal shall have an audible indicator to signal changes in its status during operation or to indicate depression of keys.
- 2-6.2.6.2 B If an audible signal is used, the signal shall not last more than 10 seconds.
- 2-6.2.6.3 B After evaluating the transaction result, a tone of 1000 Hz. +/- 5% shall be used to indicate the completion of a successful card related transaction.
- 2-6.2.6.4 B After evaluating the transaction result, a tone of 440 Hz. +/- 5% shall be used to indicate the completion of a rejected/failed transaction.
- 2-6.2.6.5 A The two frequencies used to indicate a successful transaction and a rejected/failed transaction shall not be in any form of harmony.
- 2-6.2.6.6 B The duration of the approval tone shall be 150 milliseconds +/- 10 milliseconds.
- 2-6.2.6.7 B The duration of the rejection tone shall be 500 milliseconds +/- 10 milliseconds.
- 2-6.2.6.8 A The audio signals shall be given simultaneous with the corresponding visual indication.
- 2-6.2.6.9 B The volume of the audio indicator shall be adjustable.
- NOTE:** The audio volume may be controlled by means of hardware or software functions.
- 2-6.2.6.10 C It may be possible to suppress the audio indicator.

2-6.2.7 Cardholder Keyboard

Cardholder Keyboard

- 2-6.2.7.1 C A terminal may, in addition to the PIN pad, have a Cardholder Keyboard.
- 2-6.2.7.2 A It shall be possible for the cardholder to clearly distinguish the Cardholder Keyboard from the PIN Pad, i.e. the Cardholder Keyboard shall be marked differently from the PIN Pad.
- NOTE:** This is to prevent the cardholder from accidentally entering the PIN on a keyboard other than the PIN pad, with danger of the PIN being displayed in plaintext or even worse, "snatched" by a fraudster.
- See requirements 2-7.2.2.1 page 2-7-3 to 2-7.2.2.6 page 2-7-3.
- 2-6.2.7.3 C The keyboard may allow entry of alpha characters defined for the merchants local language and other languages supported by the terminal.

2-6.2.8 PIN Pad

This section defines requirements to the physical design and security for PIN Pads. This ensures that no feasible physical

attack on the PIN Pad will disclose cryptographic keys and PINs stored in the PIN Pad. The requirements also ensure that the cardholder is able to see whether a genuine PIN Pad has been tampered with.

Keyboard Layout

- 2-6.2.8.1 A The numeric layout of the PIN Pad shall comply with the recommendations in section 4.2 of ref. 17: "EN 1332-3:2008"
- NOTE:** Referring to requirement 2-6.2.8.1, an example is given in figure 2-6.3.

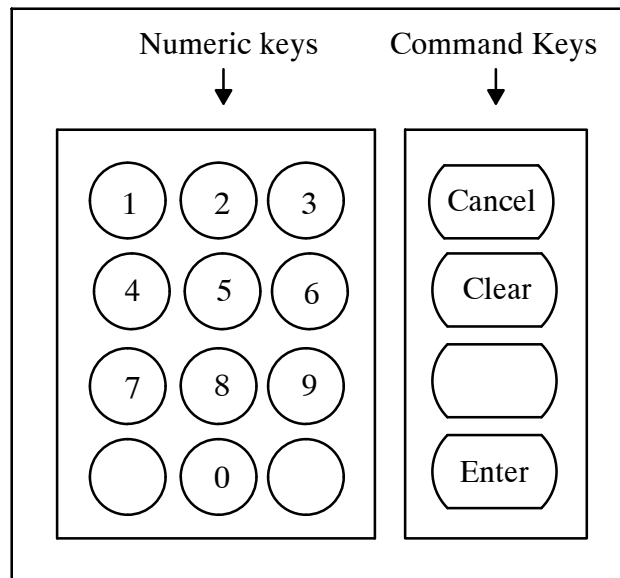


Figure 2-6.3 - Numeric Key and Command Key layout

- 2-6.2.8.2 A For PIN Pads supporting alphanumeric mapping in addition, the keyboard layout shall comply with the recommendations in section 4.3 of ref. 17: "EN 1332-3:2008".

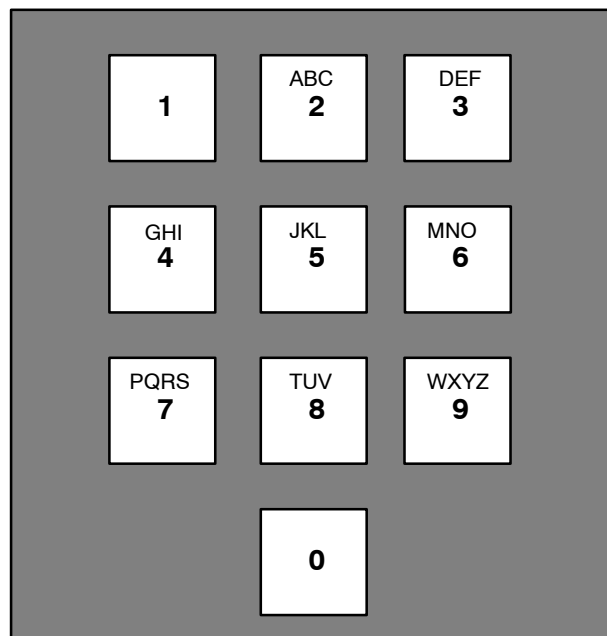


Figure 2-6.4 - Layout of Alphanumeric Keys

NOTE: Digits 1 and 0 shall not contain any alphabetic characters.

PIN Privacy

To prevent PIN value to be disclosed during entering, a number of requirements must be satisfied.

Some of these requirements concern the mechanical design of the PIN Pad itself and are defined in this section.

- 2-6.2.8.3 A Requirements concerning the privacy shielding around the PIN Pad and the actual placing of the PIN Pad when installed are defined in section 2-7 page 2-7-1 and shall be fulfilled.

General Requirements

- 2-6.2.8.4 B The keyboard/keypad and the PIN Pad shall be designed to optimize the operation from an ergonomic point of view.
- 2-6.2.8.5 B The keyboard/keypad and the PIN Pad shall have a neutral surface and be non-reflecting with a good contrast to the keys.
- 2-6.2.8.6 A It shall be possible to operate any keyboard/keypad and the PIN Pad with both the left and the right hand.
- 2-6.2.8.7 B The size of keys shall be min. 12 mm measured where the keys have the smallest length.
- 2-6.2.8.8 A The key movement for mechanical keys shall be 0.8-4.8 mm.
- 2-6.2.8.9 A The activation force for pressing a key shall comply with the recommendation in section 5.4.5 of ref. 17: "EN 1332-3: 2008".
- 2-6.2.8.10 B At depression the key top shall be over or in level with the surface.
- 2-6.2.8.11 A The terminal shall only include one PIN Pad used for all key-entering of PIN-values.

General Hardware Requirements

- 2-6.2.8.12 A The keyboard/keypad and the PIN Pad shall comply with the requirement in ref. 36: "PCI PED".

Tamper Response

- 2-6.2.8.13 B If protection against removal is required, the device shall be secured in such a manner that it is not feasible to remove it from its intended place of operation.

2-6.2.9 Command Keys

- 2-6.2.9.1 A Command Keys implemented shall have the characteristics as specified in section 4.4 of ref. 17: "EN 1332-3: 2008".
- 2-6.2.9.2 B The command keys "CANCEL" and "ACCEPT" listed in section 4.4 of ref. 17: "EN 1332-3: 2008" shall be implemented on the Cardholder Keyboard.
- 2-6.2.9.3 C The "CLEAR" key listed in section 4.4 of ref. 17: "EN 1332-3: 2008" may be implemented on the Cardholder Keyboard.

Table 2-6.1 - Command keys

Key	Functionality
“CANCEL” (Slet Alt)	Cancel the whole transaction. May as well be used for deselecting options before the actual transaction takes place.
“CLEAR” (Slet)	Erases the numeric or alphabetic character previously entered.
“ENTER” (Godkend)	Confirms an action.

2-6.2.10 Receipt Printer

- 2-6.2.10.1 B The Receipt Printer shall be capable of printing at least 24 alphanumeric characters per line.
- 2-6.2.10.2 A The printing technology and paper used (impact, laser, thermal etc.) shall assure 100% readability after proper storage of the original receipt, report or Log according to the current legislation requirements (currently 18 months).

2-6.3 Electrical Design

2-6.3.1 Introduction

Mains power may be used as the primary supply or as a secondary supply to maintain charge levels in rechargeable batteries supplying the terminal directly.

2-6.3.2 General Requirements

- 2-6.3.2.1 A The terminal shall not lose data due to power failure.
- 2-6.3.2.2 C In the event of mains failure terminal may complete a transaction in operation, including printing and logging.

It is desirable that the terminal is equipped with e.g. a battery for this purpose.

2-6.3.3 Data Store

The speed of the Data Store is very important for the overall transaction time.

- 2-6.3.3.1 B The Data Store shall be able to respond to any known Data Store command within 100 ms with a given record length of 300 bytes.

2-6.4 Software Design

2-6.4.1 Introduction

If the software is developed in a modular way, it is easier to ensure that a change in one module does not influence other modules.

Especially the software component with direct impact on the EMV level 2 kernel (e.g. Application Selection) should be segregated in a separate module(s).

2-6.4.2 General Requirements

- 2-6.4.2.1 A The requirements for the software and software development process as stated in ref. 35: "PCI DSS" and ref:37 "PCI PA-DSS" shall be fulfilled.
- 2-6.4.2.2 A It shall be possible to add and update/modify, in a secure manner, from a Terminal Operator each application software module.
- 2-6.4.2.3 A The terminal shall be able to compute the Terminal Checksum according to the data element definition in section 2-15.2.142 page 2-15-39.
- 2-6.4.2.4 A The Terminal Checksum shall follow the requirements given in ref. 23: "EMVCo Type Approval Contact Terminal Level 2 Administrative Process" and ref. 24: "EMVCo Type Approval Contactless Product Administrative Process" and related bulletins.

NOTE: Appendix B outlines the checksum rules.

2-6.4.3 Additional Requirements to the PED Software

- 2-6.4.3.1 A The software and software development of the PIN pad shall fulfill the requirements in ref: 36 "PCI PED".

2-6.4.4 Data Management

Application Independent Data Management

- 2-6.4.4.1 A The Data Store shall contain an area of at least 64 Kbytes for update commands for the PSAM.
- 2-6.4.4.2 A The Data Store shall contain an area for transactions saved in a Batch. An area of at least 128 Kbytes shall be assigned for this purpose.

Application Dependent Data Management

- 2-6.4.4.3 A The Data Store shall contain an area for update commands for software modules.

2-6.4.5 Storage of Data

Terminal Data

- 2-6.4.5.1 A The memory used for storage of non-transient data shall be non-volatile.
- 2-6.4.5.2 B The memory used for storage of data shall be able to keep data for 5 years without power.

PIN Pad Data

- 2-6.4.5.3 A The memory used for storage of non-transient data shall be non-volatile.
- 2-6.4.5.4 B The memory used for storage of data shall be able to keep data for 10 years without power.
- 2-6.4.5.5 A The PIN Pad ID shall be stored in non-volatile memory inside the PIN Pad.
- 2-6.4.5.6 A It shall be possible to load the PIN Pad ID at the PIN Pad manufacturer site before shipping the PIN Pad.
- 2-6.4.5.7 A It shall not be possible to change the PIN Pad ID once it has been loaded.

2-6.4.6 Storage of Software

Terminal Software

- 2-6.4.6.1 A The actual software version shall be stored in the terminal and it shall be possible to show it on the Cardholder Display.
- 2-6.4.6.2 A The actual hardware version shall be stored in the terminal and it shall be possible to show it on the Cardholder Display.
- 2-6.4.6.3 A The software shall be kept in non-volatile memory.
- 2-6.4.6.4 B The memory shall be able to keep data for 5 years without power.

PIN Pad Software

- 2-6.4.6.5 A The actual software version shall be stored in the PIN pad and it shall be possible to show it on the Cardholder Display.
- 2-6.4.6.6 A The actual hardware version shall be stored in the PIN pad on an electronic media and it shall be possible to show it on the Cardholder Display.
- 2-6.4.6.7 A The software shall be kept in non-volatile memory, e.g. PROM/EPROM/EEPROM or flash-PROM.
- 2-6.4.6.8 B The memory shall be able to keep data for 5 years without power.

2-6.4.7 Download Requirements

- 2-6.4.7.1 A The Terminal Supplier *or* the Terminal Operator shall be able to update the operating system, parameters and the application(s) in the terminal.

- 2-6.4.7.2 A It shall only be possible for the Terminal Supplier *or* the Terminal Operator to update the application(s), operating system and parameters stored in the MAD-Handler, however, the MAD-Handler shall update certain parameters when required to do so by the PSAM.

NOTE: The PSAM will deliver data elements to the MAD-Handler.

Terminal Software Modules

- 2-6.4.7.3 A Each module shall be upgradeable.
- 2-6.4.7.4 A Each update shall affect the software version stored in the terminal.
- 2-6.4.7.5 A The software download shall never be able to put the terminal out of business.
- 2-6.4.7.6 A No update shall be able to corrupt any data memory currently in use.
- 2-6.4.7.7 A The terminal shall ensure that the complete software update is loaded before switching to the new code.
- 2-6.4.7.8 A The download shall handle communication errors. This means that data errors during transmission shall result in data being retransmitted.
- 2-6.4.7.9 B The code to be downloaded shall be enciphered.

PIN Pad Software

- 2-6.4.7.10 A Download of software to the PIN pad shall fulfill the requirements in ref: 36 "PCI PED".

NOTE: The controller is the (one/single) entity responsible for the secure management of the Secure Cryptographic Device.

PSAM Software

It is possible to update the PSAM application when the PSAM is placed in the terminal.

- 2-6.4.7.11 A PSAM application update commands shall be saved in the same memory area as other data update commands to the PSAM.

2-6.5 Chip Card Reader Design Requirements

2-6.5.1 PSAM Card Reader(s)

- 2-6.5.1.1 B The Terminal shall have at least 4 PSAM Card Readers (PCRs).

NOTE: The PSAM Card Reader(s) may have landing contacts or sliding contacts.

- 2-6.5.1.2 A The PCR shall be able to connect to cards with physical characteristics *either* in accordance with ref. 6: "ISO/IEC 7816-1" (ID-1 format) *or* in accordance with ref. 18: "ENV 1375" (ID-000 format).
- 2-6.5.1.3 A The PCR shall be able to connect to cards with contacts placed in accordance with ref. 7: "ISO/IEC 7816-2".
- 2-6.5.1.4 B The PCR shall have a service life comparable to the service life of the terminal which it is intended for.
- 2-6.5.1.5 A Physical removal of the inserted PSAM at any time shall not leave the terminal in an invalid or unknown state.
- 2-6.5.1.6 B The shape and material of the contacting elements shall be such, that no damage is caused by them, when applied to the card; see ref. 16: "EN 726-4".
- 2-6.5.1.7 B The contact force shall be large enough to ensure contact, even in extreme environmental conditions (e.g. shocks and vibrations) which can be application dependent. However, under no circumstances shall the contact force be greater than 0.5 N per contact; see ref. 16: "EN 726-4".
- 2-6.5.1.8 C The shape of the contacts and the way of contacting the card may be done in such a way that even polluted cards are contacted properly; see ref. 16: "EN 726-4".

2-6.5.2 Electrical Interfaces

PSAM

- 2-6.5.2.1 A The CAD shall be able to supply 50 mA @ 5 V \pm 5% to each PSAM.
- 2-6.5.2.2 A The V_{pp} contact (C6) shall be electrically isolated (not connected).
- 2-6.5.2.3 A The power supply shall be decoupled directly on the contact interface (10 μ F + 100 nF).
- NOTE:** This is according to the chip manufactures.
- 2-6.5.2.4 A The power supply to the PSAM shall be short circuit proof.
- 2-6.5.2.5 A The CAD shall be able to connect electrically to the PSAM in accordance with ref. 8: "ISO/IEC 7816-3" clause 5.1.
- 2-6.5.2.6 A The CAD shall be able to control the timing on the CLK pin on the PSAM in accordance with ref. 8: "ISO/IEC 7816-3" (the default value is 3.5712 MHz).
- NOTE:** The CAD may increase the clock frequency after the ATR/PPS sequence.
- 2-6.5.2.7 A No short circuit or damage shall take place when inserting or removing the PSAM. For further explanation see ref. 8: "ISO/IEC 7816-3" clause 5.1.
- 2-6.5.2.8 A The CAD shall be equipped with a pull-up resistor according to ref. 8: "ISO/IEC 7816-3".
- 2-6.5.2.9 A The time constant controlling the rise time of the signal on the I/O pin shall not be greater than 500 ns with the ICC inserted.

- 2-6.5.2.10 A The CAD shall be able to handle the PPS dialog in accordance with ref. 8: "ISO/IEC 7816-3".
- 2-6.5.2.11 C The CAD should select the fastest parameters given in the ATR if possible. In case no parameters are given in the ATR from the PSAM the CAD should try with its fastest parameters.

Cardholder ICC

- 2-6.5.2.12 A The CAD shall be compliant to the electrical interfaces as specified in ref: 20 "EMV ICC Specification, Book 1".
- 2-6.5.2.13 A The V_{pp} contact (C6) shall be electrically isolated.
- 2-6.5.2.14 A The power supply shall be decoupled directly on the contact interface ($10 \mu F + 100 nF$).

NOTE: This is according to the chip manufactures.

- 2-6.5.2.15 A The time constant controlling the rise time of the signal on the I/O pin shall not be greater than 500 ns with the ICC inserted.
- 2-6.5.2.16 A The CAD shall be able to control the timing on the CLK pin on the Card in accordance with ref. 8: "ISO/IEC 7816-3", the default value is 3.5712 MHz .
- 2-6.5.2.17 C The CAD may increase the clock frequency after the ATR sequence.
- 2-6.5.2.18 A The CAD shall be able to handle the PPS dialog in accordance with ref. 8: "ISO/IEC 7816-3".
- 2-6.5.2.19 C The CAD should select the fastest parameters given in the ATR if possible. In case no parameters are given in the ATR from the PSAM the CAD should use default parameters.

Merchant Application

NOTE: The protocol between the terminal and the Merchant Application is out of scope for this specification.

2-7 Privacy Shield on PIN Entry Devices

2-7.1 Introduction

The scope of this section is to provide the security requirements for a terminal including a PIN Entry Device in order to minimize the risk of unintended compromise of the PIN code and/or card data from the magnetic stripe.

This section shall be seen as a supplement to the general requirements for terminals accepting PIN codes.

It is intended that the requirements defined shall be objective and measurable.

The requirements for the privacy shield around the PIN Entry Device are defined, as well as the requirements concerning the placement and setting up of the terminal.

Additional requirements for the design and construction of unattended terminals are defined too, with the purpose of minimizing the risk of placing a Tapping Device for the magnetic stripe Card Data.

A number of recommendations for the design and placement of the terminals are stated in this specification.

2-7.1.1 Terminology

Authorized Person,	a person who shall be allowed to access the interior of the terminal. Only persons who needs to access the interior of the terminal as part of the job shall be authorized to do so.
Card Data,	the complete data contents (track 2) of the magnetic stripe on the Card.
Shoulder Surfing,	the situation when a PIN is compromised as a result of visual pick up while the PIN is entered.
Tapping Device,	a physical device placed in connection with either the PIN Entry Device or the Card Reader for mechanical and/or electronic collection of data.

2-7.2 Privacy Shield around the PIN Entry Devices

2-7.2.1 Shielding - Size and Orientation

The size and orientation of the privacy shield around the PIN Entry Device shall ensure that the angles from which Shoulder Surfing may be possible is limited to an absolute minimum.

- 2-7.2.1.1 A In a circle segment of at least 270 degrees, with the opening towards the cardholder, a privacy shield shall be placed.

The center of the circle segment shall be the center of the '5'-key.

See figure 2-7.1 page 2-7-8.

NOTE: The privacy shield does not need to be designed as a circle segment, but the shield shall cover the PIN Entry Device as if the shield was shaped as a circle segment.

NOTE: The shield may be omitted on parts of the circle segment if the design of the terminal guarantees the same level of privacy within the specified circle segment of 270 degrees.

- 2-7.2.1.2 A Within the specified circle segment of 270 degrees seven 'reference directions' are defined. The seven 'reference directions' are named *a*, *b*, *c*, *d*, *e*, *f* and *g*.

The angles between the 'reference directions' shall be 45 degrees as defined in figure 2-7.2 page 2-7-9.

The height of the privacy shield in the 'reference directions' *b*, *d* and *f* shall guarantee that the angle between the level of the key-tops and the top of the shielding shall be 45 degrees at least.

The height of the privacy shield in the 'reference directions' *a*, *c*, *e* and *g* shall guarantee that the angle between the level of the key-tops and the top of the shielding shall be 35 degrees at least.

The height of the privacy shielding between the 'reference directions' shall not be lower than the height defined by a straight line between the 'reference points' (see figure 2-7.3)

NOTE: The angle defining the height of the shielding shall be measured from the center of the surface on the '5'-key to the top of the shield.

NOTE: If the design of the terminal guarantees the same level of privacy, e.g. due to construction of the housing of the terminal, no dedicated privacy shield will be required on the actual parts of the circle segment.

- 2-7.2.1.3 A The shielding shall be built in a non-transparent material.

- 2-7.2.1.4 C It shall not be easy to remove the privacy shield around the PIN Entry Device, and if the shield is removed due to vandalism, the shielding shall be easy to reestablish by the supplier of the terminals or by a service agent.

2-7.2.2 PIN Entry Device and Additional Numeric Keys

If the terminal includes both a PIN Entry Device and an additional Cardholder numeric keyboard the layouts shall be strikingly different to prevent the cardholder from accidentally entering the PIN-code on the numeric keyboard.

- 2-7.2.2.1 B If an additional set of Cardholder numeric keys (0-9) is included on the Cardholder operated part of the terminal, then these keys shall be mounted with a strikingly different design and position compared to the PIN Entry Device.
- NOTE:** This requirement may be complied with by e.g. showing the guiding messages (Enter PIN, etc.) on a display in connection with the PIN Entry Device, while the display used for selecting goods and/or services is just showing a message like "Perform payment".
- 2-7.2.2.2 B The keys themselves within an additional set of numeric keys shall appear strikingly different to those on the PIN Entry Device.
- 2-7.2.2.3 B The additional set of numeric keys shall clearly be marked with the purpose of the use of these keys.
- 2-7.2.2.4 B If an additional set of numeric keys is included on the terminal, the PIN Entry Device shall clearly be marked with the message "Only PIN Codes" (kun PIN-koder).
- 2-7.2.2.5 B A warning saying "Protect your PIN-Code" (Beskyt din PIN-kode) shall either appear on the display when PIN entry is awaited or the message shall appear on a permanent label near to the PIN Entry Device.
- 2-7.2.2.6 B If an additional set of numeric keys is included on the terminal, these keys shall be placed to the left of the PIN Entry Device.

2-7.3 Shielding - Design Recommendations

2-7.3.1 Introduction

This section defines a number of design recommendations, which may be a help in the process of designing an optimal privacy shielding.

- 2-7.3.1.1 C The shielding should at least cover the PIN keys. The shield may as well cover the command : "Cancel", "Clear" and "Enter".
- 2-7.3.1.2 C The shielding and the cardholder's body are intended to protect against Shoulder Surfing from all angles.
- 2-7.3.1.3 C The shielding shall allow for use by both right-handed and left-handed cardholders.

- | | | |
|------------|---|------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-7.3.1.4 | C | The shielding shall take into account the size of the cardholders hand. |
| 2-7.3.1.5 | C | The shielding should allow the operation of the terminal, when the terminal is placed in the intended height and angle towards the cardholder. |
| 2-7.3.1.6 | C | The shielding may not limit the use depending on the light. |
| 2-7.3.1.7 | C | The shielding may not cover the PIN keys for the cardholders view, when the cardholder is not covering the PIN keys by the hand. |
| 2-7.3.1.8 | C | The shielding may not limit the operation of the Card Reader, functions key or other operations of the terminal. |
| 2-7.3.1.9 | C | The shielding should be constructed to operate in the environment for which the terminal is intended. |
| 2-7.3.1.10 | C | The shielding should be robust and easy to clean. |
| 2-7.3.1.11 | C | The shielding should be considered as an integrated part of the 'total design' of the terminal. |
| 2-7.3.1.12 | C | The design of the shielding should be simple and harmonically. |
| 2-7.3.1.13 | C | The shielding should signal that the use of the terminal is easy and confident. |

2-7.4 Protected access to Card Reader and PIN Entry Device

When the access to the inside of a terminal is free, it may be possible to place a tapping device on the Card Reader.

Especially terminals placed and used in an unattended environment may be exposed to such an attack from unauthorized persons.

To minimize this risk, a number of requirements concerning the access to the interior of the terminals are defined.

The requirements and recommendations defined in this section are targeted at Unattended terminals for which they are mandatory, but the requirements may be implemented on Attended terminals, too.

2-7.4.1 Access to the interior of the terminal

Only persons who are authorized to service the terminal shall be able to open an Unattended terminal. The access to the Card Reader, Card Data and the mounting of the PIN Entry Device shall be protected.

The terminal may be designed and constructed with separate access to the area within the terminal, which requires normal and frequent access for maintenance purposes, e.g. to the receipt printer.

If the area which requires normal and frequent access is separated from the area where Card Reader, Card Data and PIN Entry Device is accessible, the security functions may also be separated.

- 2-7.4.1.1 A The access to the interior of an Unattended terminal shall be protected by a 'lock', and the 'key' shall only be issued to Authorized Persons.

NOTE: The 'interior of an Unattended terminal' is defined as the area where the Card Reader or Card Data is available, and the area where the mounting of the PIN Entry Device is accessible.

NOTE: The 'lock' and 'key' may be implemented using technologies other than a physical lock and key. Other implementations which ensure a similar level of security may be accepted.

- 2-7.4.1.2 B The terminal cabinet shall be locked, even when the terminal is not in use.

- 2-7.4.1.3 A A switch or similar equipment shall be installed to detect when the Unattended terminal is opened and closed.

NOTE: The switch shall detect when access to the area with the Card Reader, Card Data and the PIN Entry Device is possible.

- 2-7.4.1.4 A The switch (or similar equipment) installed to detect whether the Unattended terminal is open or closed, shall also be able to detect when an unauthorized entry to the interior of the terminal has been forced, e.g. by breaking the lock.

- 2-7.4.1.5 A Each time the Unattended terminal is opened a message shall be recorded in the log of card transactions. The message shall at least include information about the date and time, and an indication defining that the terminal has been opened.

- 2-7.4.1.6 C Each time the Unattended terminal is closed a message may be recorded in the log of card transactions. The message should at least include information about the date and time, and an indication defining that the terminal has been closed.

- 2-7.4.1.7 A If an unauthorized entry to the interior of the Unattended terminal has been forced, otherwise than picking the 'lock', physical damages shall be visible on the outside of the terminal.

NOTE: The design and construction of an unattended terminal must consider that no screws (or similar) are

available from the outside of the terminal, if the removal of these screws (or similar) make access to the interior of the terminal possible.

- 2-7.4.1.8 C The mounting of the Card Reader should prevent the installation of a Tapping Device on the front of the Card Reader.

NOTE: The front of the Card Reader visible from the outside of the terminal should prevent that a Tapping Device should be fixed or just clicked to the front.

2-7.4.2 No operation when the terminal is open

The terminal shall not be able to operate when the terminal is open, and after closing the terminal the operation shall be re-enabled manually by an Authorized Person.

- 2-7.4.2.1 A When the Unattended terminal is open, the normal operation of the terminal shall be disabled.

NOTE: When the switch or similar equipment installed has detected that the terminal is open, the normal operation shall be disabled and a message on the display shall indicate this to the cardholder.

- 2-7.4.2.2 A When the Unattended terminal has been opened the normal operation shall remain disabled until the terminal is closed again, and an Authorized Person has re-enabled the operation.

- 2-7.4.2.3 A When the normal operation for an Unattended terminal is disabled the Card Reader shall not read cards.

NOTE: If a motorized card reader is used, the motor shall be reversed immediately if a card is inserted.

- 2-7.4.2.4 A The re-enabling of the Unattended terminal for normal operation shall only be possible for Authorized Persons.

NOTE: The re-enabling may e.g. be performed by entering a User-ID and a Password. Other implementations which ensure a similar level of security may be accepted.

- 2-7.4.2.5 A Each time the Unattended terminal is re-enabled, a message shall be recorded in the log of card transactions. The message shall at least include information about the date and time, and an indication defining that the terminal has been re-enabled.

- 2-7.4.2.6 C If e.g. an User-ID is identifying the Authorized Person when re-enabling an Unattended terminal, it is recommended that this information is included in the log.

2-7.4.3 Other Equipment

The access to card data shall also be protected when the card data is present in other equipment than the terminal, e.g. if card data is present in a control-system placed in a separate unit or in a separate building.

Also the cabling between separate units shall be protected.

The requirements defined in this section may not be possible to comply when the terminal or the system is designed, because the level of compliance may be a result of the installation and placement of the terminal and other equipment at the Merchant. But during the design and development of a terminal these requirements shall be considered.

- 2-7.4.3.1 A If the Card Data (full magnetic stripe information) is present in other equipment than the Unattended terminal, the access to this equipment shall be protected by a 'lock' and the 'key' shall only be issued to Authorized Persons.

NOTE: The 'lock' and 'key' may be implemented using technologies other than a physical lock and key. Other implementations which ensure a similar level of security may be accepted.

NOTE: If the equipment, in which the card data are present, is placed in a building separated from the unattended terminal, the access to this equipment is considered as 'locked' if the area is either attended or the building is locked when not attended.

- 2-7.4.3.2 A If the Card Data (full magnetic stripe information) is transmitted between the Unattended terminal and other equipment, the cables used shall not be accessible or visible without making damages to the terminal or the construction made to protect the cabling.

NOTE: Unattended persons must not be able to open any switch- or connect-boxes without making damage, if the card data is transmitted through the boxes.

2-7.5 Figures

2-7.5.1 Privacy Shield around the PIN Entry Device

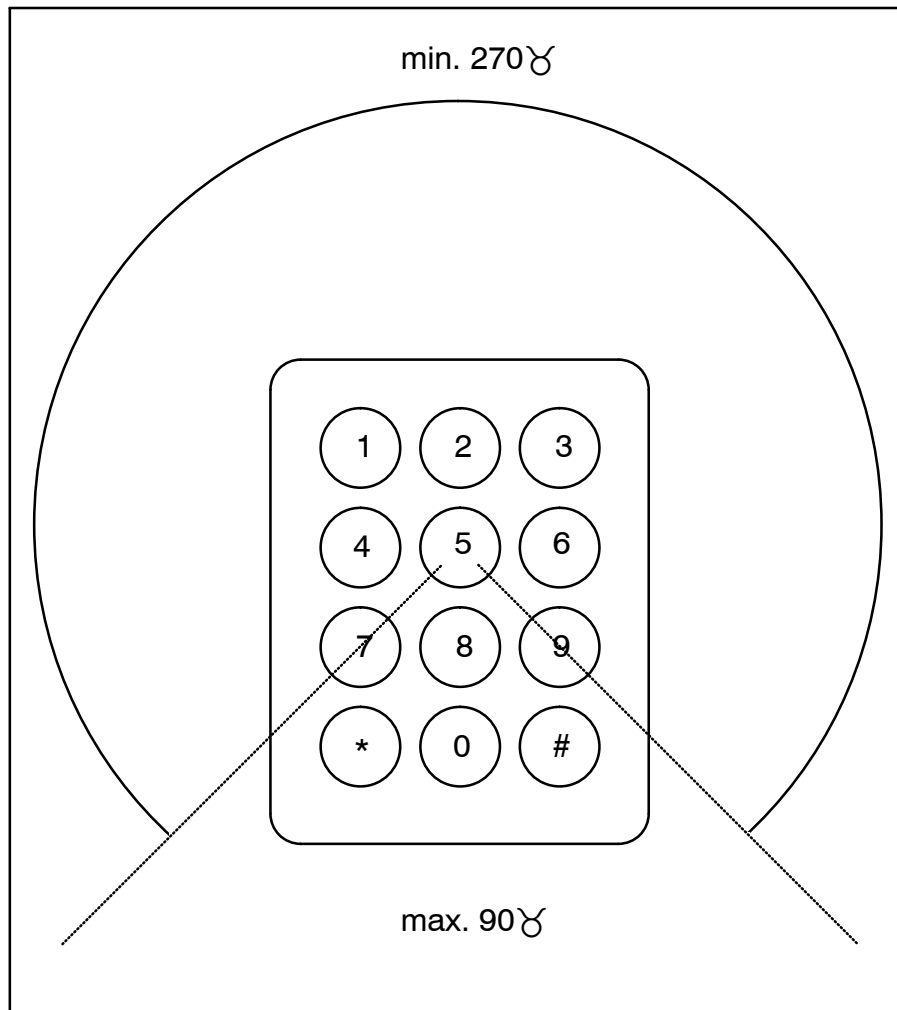


Figure 2-7.1 - Privacy Shield around the PIN Entry Device

2-7.5.2 Reference Directions

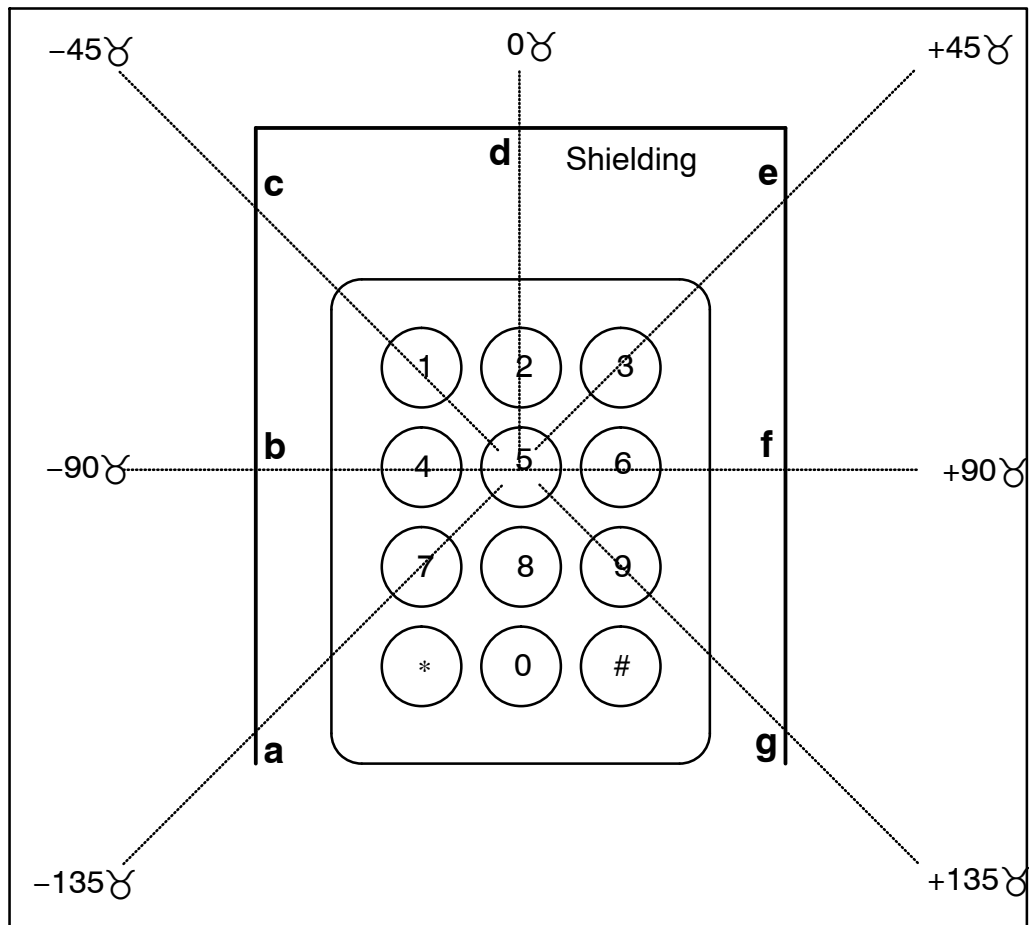


Figure 2-7.2 - Reference Directions - a, b, c, d, e, f and g

2-7.5.3 The Height of the Shielding

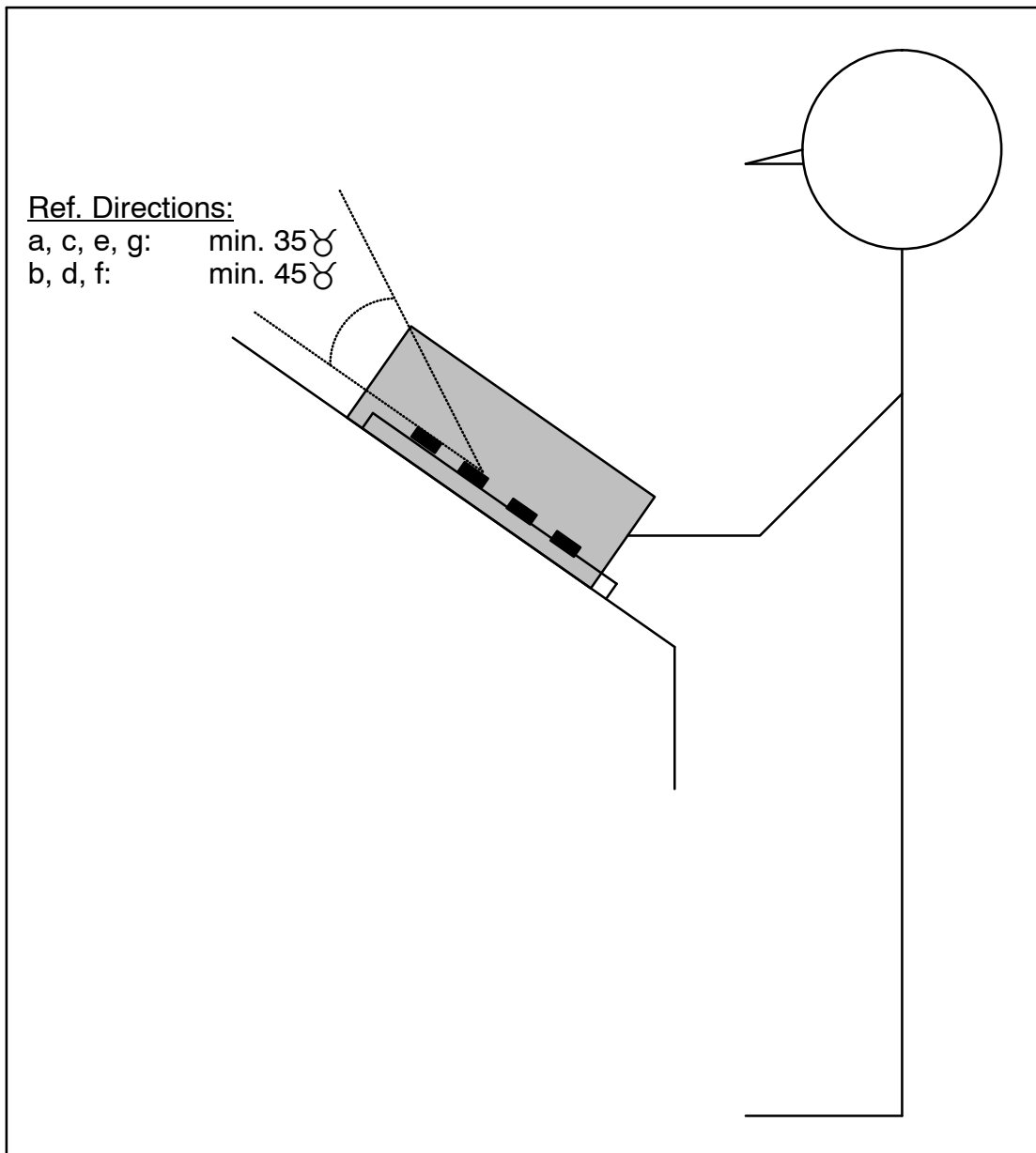


Figure 2-7.3 - The Height of the Shielding

2-7.5.4 Mounting of the PIN Entry Device (Angle)

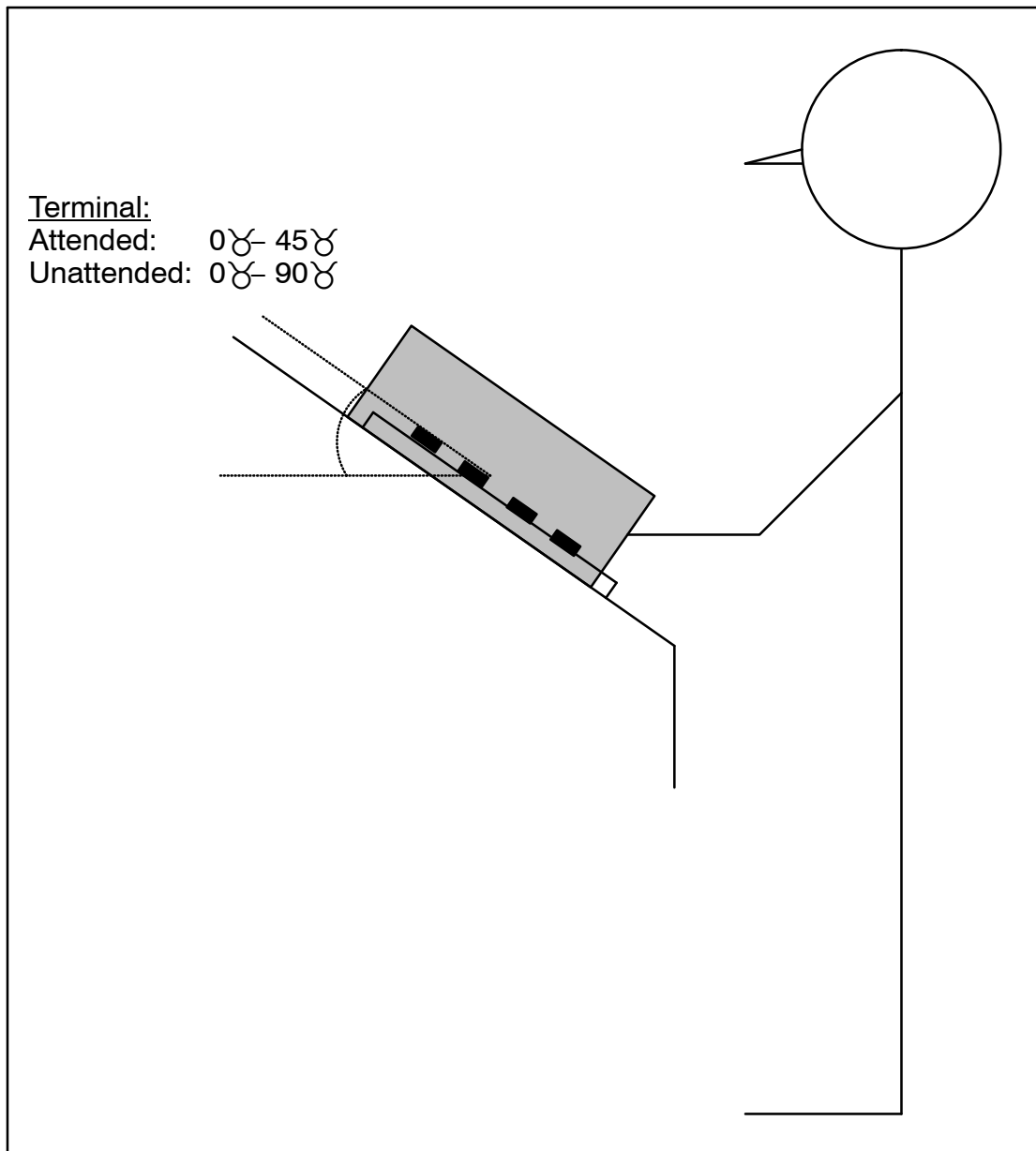


Figure 2-7.4 - Mounting of the PIN Entry Device (Angle)

2-7.5.5 Height and position of the PIN Entry Device

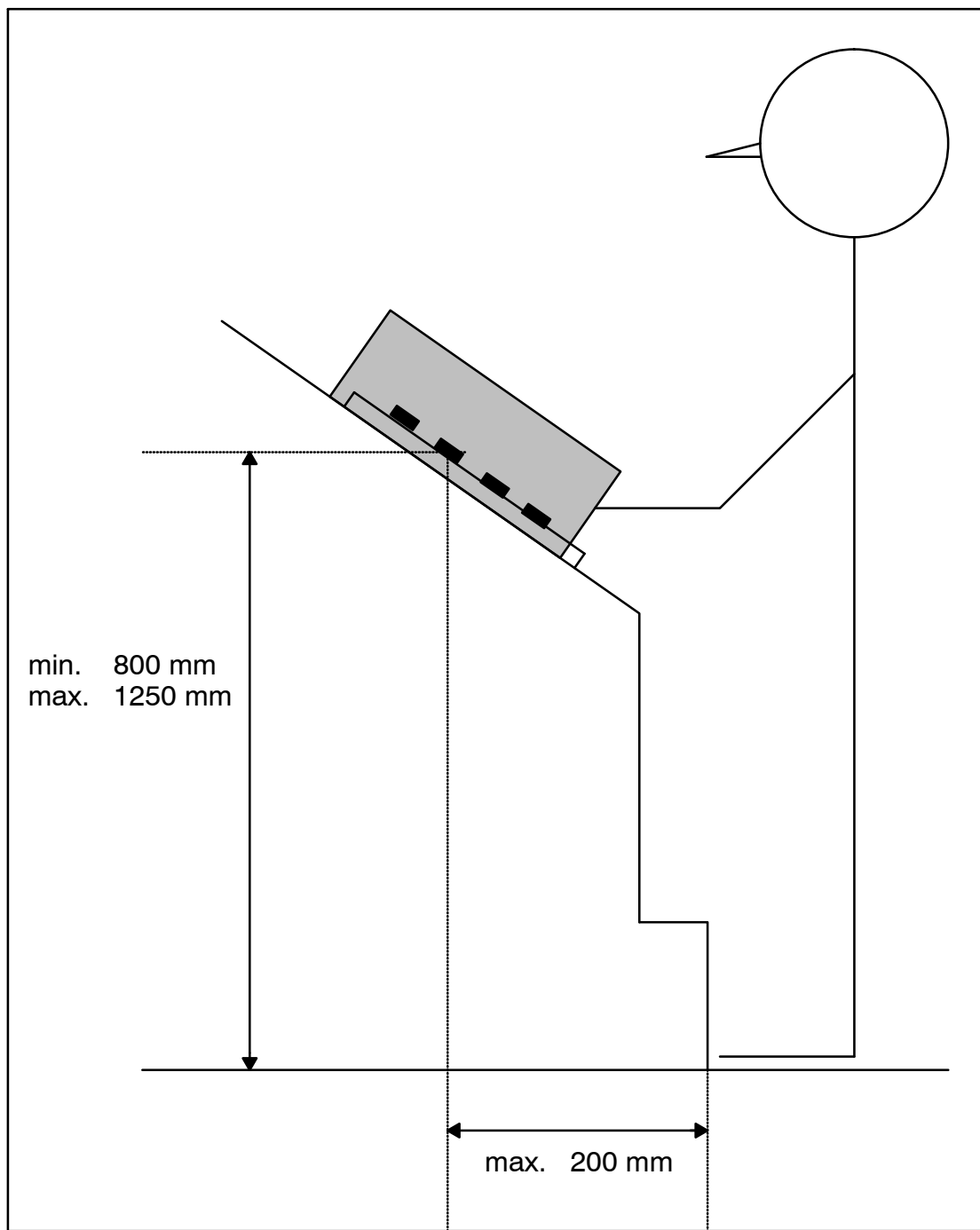


Figure 2-7.5 - Height and Position of the PIN Entry Device

2-8 Service Packs

2-8.1 Introduction

In order to open for new variants of commands/responses, Service Packs have been introduced.

Typically, new requirements and data elements which were not known at the initial system design phase have become necessary.

2-8.2 Selection of Service Packs supported

The PSAM will always support the baseline command set i.e. no Service Packs supported. New PSAM versions may support several Service Packs.

Selection of a Service Pack is done in the start up phase. See section 2-5.1.3 (Restart).

A Service Pack is requested by the terminal as part of the Terminal Approval No. which is exchanged in the *Exchange Debit/Credit Static Data Information* command after finding the mutually supported Service Pack No. using the *Get Debit/Credit Properties* command.

If the PSAM does not support the Service Pack requested, the terminal will interrupt/terminate the start-up procedure.

NOTE: As of TRG-OTRS version 3.x and later only terminals supporting Service Pack 2 or higher are applicable. Information on previous Service Packs is greyed out and only included for informational purpose.

2-8.2.1 General requirements

As specified in requirement 2-5.1.3.11 page 2-5-7, the terminal must support at least Service Pack 2.

See also section 1-9.7 page 1-9-3 Service Packs

2-8.2.2 Terminal - Terminal Approval No.

In the data element Terminal Approval No., the 3 most significant bits is now used as Service Pack No.

- 2-8.2.2.1 A When configuring the terminal, the 3 most significant bits of the Terminal Approval No. shall be configured according to which Service Pack the terminal is requesting. See section 2-15.2.141 page 2-15-38, Data Elements.

2-8.3 Service Packs Overview

Table 2-8.1 show the relationship between Service Packs and commands, data elements & functions.

Table 2-8.1 - Service Packs Overview

Functionality		Service Packs		
Commands		Baseline	SP1	SP2
Initiate Payment		☞	☞	
Initiate Payment 2				☞
Get Amount		☞		
Get Amount 2			☞	
Get Amount 3				☞
Validate Data		☞		
Validate Data 2			☞	☞
Get Debit/Credit Properties				
Identifier	'0001' – '0007' ¹⁾	☞	☞	☞
	'0008'			☞
Set Debit/Credit Properties				
Identifier	'8000'			☞
	'8001' – '8002' ¹⁾	☞	☞	☞
Functionality				
MSC PIN retry			☞	☞
Issuer Envelope Data				☞
Account Type				☞
Message size (up to 512 bytes)		☞	☞	
Message size (up to 1024 bytes)				☞
Legend:				
1) = Earlier versions of the PSAM may not be able to respond successfully to all identifier values.				

2-8.4 Service Pack No. 1

Service Pack No. 1 comprises a number of new formats, including new variants of existing commands and responses. The commands/responses affected by Service Pack No. 1 are:

- *Get Debit/Credit Properties*, a new set of response data is defined.
- *Get Amount 2*, a new and extended variant of the existing command *Get Amount*.
- *Validate Data 2*, a new and extended variant of the existing command *Validate Data*.

Service Pack No. 1 will also enable the use of the function "PIN Retry".

2-8.4.1 MSC PIN Retry

PIN Retry is a function for re-entering the PIN after an online PIN validation has failed.

During PIN retry the cardholder is requested to re-enter the PIN, without entering/swiping the card again.

Service Pack No. 1 enables this function, by letting the PSAM include a new host request in the response to the *Validate Data 2* command.

The description of PIN retry may be found in section 2-5.16.5 page 2-5-119 Host Declined Transactions (Requests).

2-8.4.2 Get Amount 2

If the transaction amount has been omitted in the *Initiate Payment command*, the PSAM will issue a *Get Amount* command to obtain the actual amount(s).

Service Pack No. 1 includes the data element PAN-prefix (containing the first 8 digits in the PAN) to be included as discretionary data in the command message. The PAN-prefix may e.g. be used for calculating any additional merchant specific surcharges/fees to be added before the amount is transferred to the PSAM.

Service Pack No. 1 also implies an extension of the response to *Get Amount 2*. The response shall include both the Transaction Amount and Amount Other.

Issuing the Get Amount 2 Command Twice

The *Get Amount 2* command may be issued twice depending of the actual EMV card.

The EMV card may request the amount in an early stage of the transaction and before the PAN is known e.g. if requested in the PDOL returned in the Select command.

In this situation the PAN-prefix indicated in the *Get Amount 2* command will be set to '00 00 00 00'.

If the terminal assumes that the PAN-prefix should be known before the amount can be determined, the terminal may gen-

erate a response to the *Get Amount 2* command containing Response Code 'FFF2' (time-out).

The Response Code 'FFF2' returned will indicate to the PSAM that the transaction shall continue if the PAN-prefix was '00 00 00 00' in the command. This Response Code will also imply that a second *Get Amount 2* command shall be issued later on during the transaction, after the PAN is known.

If a successful response to *Get Amount 2* is returned (including the amount) the PSAM will not issue any additional *Get Amount 2* command.

- 2-8.4.2.1 C If the *Get Amount 2* command during an EMV transaction contains the value '00 00 00 00' in the PAN-prefix field, the terminal may respond "the amount not yet known" by returning the Response Code 'FFF2' (time-out).

NOTE: If a Cancellation is initiated as defined in requirement 2-5.16.10.3 page 2-5-123, the Merchant Interface shall insert the Response Code 'FFF2' in *all* subsequent responses to *Get Amount 2* command.

See table 2-8.2 page 2-8-7 for comparison of the different variations of the *Get Amount* command.

2-8.4.3 Validate Data 2

The response to *Validate Data 2* returns a number of additional data elements.

The following data elements are added in the response:

- **Action Code_{PRINT}:** indicating the Action Code to be printed on the receipt.
- **Approval Code:** indicating the Approval Code to be printed on the receipt.
- **Authorization Response Code:** indicating the value to be printed on the receipt.
- **POS Entry Mode:** indicating the actual value. For Token based transactions, the Token includes information about the card technology used. If the card technology used is MSC (Token Format = 'D4') the magnetic stripe may have been read as fallback from ICC. To be able to distinguish between the two different situations:
 - Magnetic Stripe Track 2 and
 - Magnetic Stripe Track 2 as fallback for ICC
 The terminal shall extract this information from position 3 (value = '7' (Magnetic stripe read after ICC malfunction)) of POS Entry Mode (returned by the PSAM). See table 2-13.89 on page 2-13-70 for further details.
- **CVM Status:** indicating the type(s) of CVM performed, in combination with online/offline authorization. An EMV transaction may initially request an online authorization, and the CVM Status stated in the response to the EMV Payment command will indicate "Authorization: Online". If the online request fails, the transaction may be complete offline successfully. CVM Status stated in the response to *Validate Data 2* will indicate the 'final transaction information'.

2-8.5 Service Pack No. 2

Service Pack No. 2 comprises a number of new formats, including new variants of existing commands and responses. The commands/responses affected by Service Pack No. 2 are:

- A new format of the *Initiate Payment* command (denoted *Initiate Payment 2*) for EMV, MSC and Token based transactions. This is done to accommodate the new EMVCo data element "Account Type".
- *Get Debit/Credit Properties*, a new set of response data is defined in order to indicate the maximum length of data that can be conveyed from the terminal to the issuer in the new "Issuer Envelope" functionality.
- *Get Amount 3*, a new and extended variant of the command *Get Amount*
- *Set Debit/Credit Properties*, a new command has been introduced to convey terminal specific data to the PSAM.

2-8.5.1 Get Amount 3

The following data elements are added to the *Get Amount 3* command and response message compared to the original *Get Amount* command:

Command:

- Primary Account Number (PAN)
- PAN Sequence No.
- Amount Request

Response:

- Amount Other
- Amount Status

Issuing the Get Amount 3 Command Twice

The *Get Amount 3* command may be issued twice depending of the actual EMV card.

If the EMV card request the amount before the terminal/PSAM has read the card data, the terminal is not able to determine the actual card brand. Therefore, the terminal/cash-register system is not capable of computing the accurate amount as surcharges etc. is often brand specific.

With the new *Get Amount 3* command, the PSAM will in this case request an initial amount (the amount without any surcharges). If an estimated amount is obtained, the PSAM will request the amount again at a later state, but this time the accurate amount.

When the final amount is requested, the PSAM will convey the full PAN and PAN Sequence No. to the terminal/cash register system, making it possible to compute the accurate amount.

When the PSAM request the final amount, the terminal/cash register system shall return the accurate amount, otherwise the transaction will be rejected.

See table 2-8.2 page 2-8-7 for comparison of the different variations of the *Get Amount* command.

NOTE: While it for the *Get Amount 2* command was possible to return the Response Code equal to 'FFF2' (time-

out) if the amount was not ready, the *Get Amount 3* command requires that the requested amount (initial or final) is returned.

2-8.5.2 Message Size

When Service Pack 2 is supported, the Request- and Advice-messages generated by the PSAM may exceed 512 bytes. Therefore, the terminal shall be able to process messages up to 1024 bytes.

The actual requirement can be found in ref. 28: "TAPA Errata".

Table 2-8.2 - PSAM Behavior for Variants of different *Get Amount* Commands

Command			Command data			Response data		Transaction process	
			PAN		Amount Request	Amount	RC		
			Prefix	Full PAN					
1	Get Amount	1st issue				Amount	Successful	Amount entry finished	
							Time-out	Go to step 2	
							Other	Rejected	
2		2nd issue				Amount	Successful	Amount entry finished	
							Other	Rejected	
3	Get Amount 2	1st issue	Absent			Amount	Successful	Amount entry finished	
							Time-out	Go to step 4	
							Other	Rejected	
			Present			Amount	Successful	Amount entry finished	
							Time-out	Rejected	
							Other	Rejected	
4		2nd issue	Present			Amount	Successful	Amount entry finished	
							Other	Rejected	
5	Get Amount 3	1st issue		Absent	Initial	Estimated	Successful	Go to step 6	
						Accurate	Successful	Amount entry finished	
							Other	Rejected	
						Final	Estimated	Successful	Rejected
							Accurate	Successful	Amount entry finished
								Other	Rejected
				Present		Initial	Estimated	Successful	Go to step 6
							Accurate	Successful	Amount entry finished
								Other	Rejected
						Final	Estimated	Successful	Rejected
							Accurate	Successful	Amount entry finished
								Other	Rejected
6		2nd issue		Absent	Final	Estimated	Successful	Rejected	
						Accurate	Successful	Amount entry finished	
							Other	Rejected	
				Present		Estimated	Successful	Rejected	
						Accurate	Successful	Amount entry finished	
							Other	Rejected	

Legend:
 RC = Response Code, 1st issuer/2nd issue = first/second time the *Get Amount* command is sent to Merchant Application during a transaction. Other = Response Codes relevant for the *Get Amount* command, not mentioned specifically above. Grey boxes mean not applicable.

2-8.5.3 Issuer Envelope Functionality

For issuers, where issuer specific data entered at the terminal are requested to be conveyed transparently to the issuer, the new Issuer Envelope functionality may apply. The envelope functionality is applicable for EMV, MSC and Token based transactions.

The terminal can use the new *Set Debit/Credit Properties* command to send the data to the PSAM. The PSAM will then add the data to the APACS messages generated.

Data to be send using the envelope functionality shall be available for the PSAM in the time slot after the *Initiate Payment* response and before the *Complete* command.

The Issuer Envelope Data delivered to the PSAM will be included in all the subsequent APACS messages, until one of the following conditions are met:

- A new Issuer Envelope Data is delivered to the PSAM
- An "empty" Issuer Envelope Data field is delivered to the PSAM (LEN_{IED} = '00')
- The *Complete* command is processed

Issuer Envelope Data will be conveyed in field 47 (tag TX) while Issuer Envelope Response Data (if present) are conveyed in field 44 (tag TY).

It will therefore be possible for the merchant to send certain data in the request and e.g. send other data (or reset the data by setting the length of data equal to 0) in the advice.

For MSC transactions, Issuer Envelope Data shall be available before just after the *Initiate Payment* response, if the data are going to be delivered in the Financial Request.

As the space for this issuer specific data are limited in the PSAM, the maximum number of bytes to be used in the envelope functionality (for the PSAM in question) can be obtained by use of the *Get Debit/Credit Properties* command (with the Identifier = '0008').

2-8.5.4 Initiate Payment 2 / Account Type

The purpose of the data element Account Type is stated in ref. 20: "Specification Update Bulletin No. 39: Definition of the new data element: Account Type".

A new version of the *Initiate Payment* command (denoted *Initiate Payment 2*) has been defined in order to make it possible to indicate the Account Type.

- 2-8.5.4.1 A The value shall be set to the default value ('00') until further notice.

2-9 Merchant Initiative Bypass

2-9.1 General

2-9.1.1 Introduction

Merchant Initiative Bypass is a functionality supported in OTRS, which makes it possible for the merchant to “force” a certain CVM (PIN, signature or No CVM) and/or online/preferred offline/offline when a transaction is initiated.

If the Merchant does not “force” any of the above mentioned possibilities, the PSAM will automatically select the CVM and online/offline determined by the rules implemented in the PSAM.

In case of forced CVM and/or online/offline the rules implemented in the PSAM will still be the master. This means that the PSAM will decide whether the transaction shall be accepted or rejected due to the Merchant Initiative Bypass selected.

In case of preferred offline, this is only a preferred condition instead of a forced condition, i.e. the PSAM will just bypass it, if not allowed.

Implementing Merchant Initiative Bypass functionality has only impact on the terminal.

Figure 2-9.1 below gives an overall view of how the Merchant Initiative Bypass can be implemented.

The most obvious implementation of Merchant Initiative Bypass functionality is probably when magnetic stripe cards is used and altering from PIN (default) to signature.

But the proposed solution will be usable:

- Independently of the card technology
- Independently of the “force” parameters used.

It will be up to the terminal manufacture to decide which “force” parameters that shall initiate Merchant Initiative Bypass just as if this functionality shall be implemented at all.

2-9.1.2 General Requirements

If the Merchant Initiative Bypass functionality is going to be implemented, the implementation must comply to the following requirements:

- | | | |
|-----------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-9.1.2.1 | C | When Merchant Initiative Bypass is initiated, the current transaction in progress shall be interrupted as if the merchant activated the Cancel Key. |
| 2-9.1.2.2 | C | Merchant Initiative Bypass shall only be possible while the <i>Initiate Payment</i> command is in progress. |

- 2-9.1.2.3 C When Merchant Initiative Bypass is initiated, the cardholder shall be informed (via the cardholder display) that the transaction is not rejected, but continues.
- 2-9.1.2.4 C Taken requirement 2-9.1.2.3 into account, the Message Code '87' ("Cancellation") shall be substituted by the Message Code '64' ("Retrying").
- 2-9.1.2.5 C Merchant Initiative Bypass shall only be initiated by the merchant and only be continued if the ASW1-ASW2 returned from the PSAM indicates that this is the reason for interrupting the current transaction.
- 2-9.1.2.6 C When ICC transactions are performed, the ICC should be reset (power off/on) in order to initiate a new transaction seen from the ICC (and PSAMs) view. As outlined in figure 2-9.1 page 2-9-3, application selection can be "skipped" in the following way:
- Creation of the Candidate List can be skipped (the existing Candidate List is still valid)
 - The terminal can directly select the application previously selected.

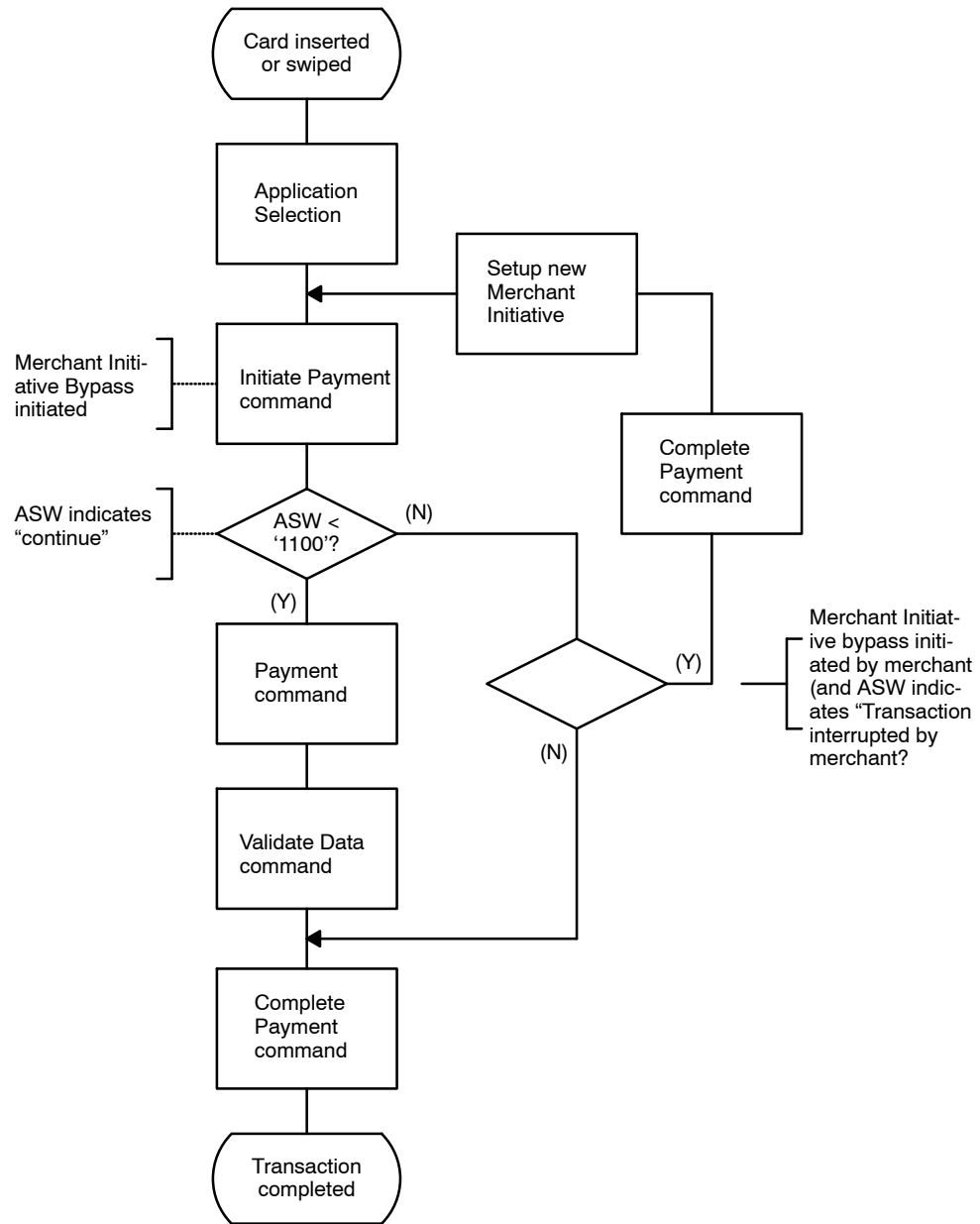


Figure 2-9.1 - Merchant Initiative Bypass

This page is intentionally left blank

2-10 Additional Transaction Information

2-10.1 Introduction

In a number of payment situations, the need for adding information to a specific transaction may arise.

This section specifies two methods to use when transmission of such additional transaction information is used in a terminal developed according to this specification.

2-10.2 Flex Terminals and Transaction Information

The additional transaction information is defined by the card issuer and/or acquirer, and is generated by the terminal for inclusion in the transactions sent to the card issuer/acquirer.

The additional information is regarded as discretionary data by the PSAM and the transaction acquiring system. The information is not intercepted and verified during transmission to the acquirer / issuer processing, nor is any response from the acquirer / issuer validated before it is sent back to the terminal.

The functionalities requires the usage of Service Pack 2 commands and responses.

Generation and/or processing of additional transaction information is outside the scope of this specification. Other sections in this specification defines application specific data or country specific data to be placed in the additional transaction information.

There are two ways of handling additional transaction information, the previously defined method using the Issuer Envelope and a new method using the Extended Issuer Envelope.

The access to the envelopes is possible using the Set D/C properties (section 2-14.5.9) and Get D/C Properties (section 2-14.5.8) commands. See as well section 1-10.5.2 for more information.

Figure 2-10.1 page 2-10-3 depicts how the transaction flow in the terminal is augmented.

The commands are only used when needed.

NOTE: The size of data is currently limited to 150 bytes for MSC transactions and to 100 bytes for EMV transactions.

2-10.2.1 Terminal requirements

- 2-10.2.1.1 A The terminal shall be Service Pack 2 compatible in order to support Additional Transaction Information.
- 2-10.2.1.2 A The terminal shall - during power on - request the use of Service Pack 2 as described in section 2-8, "Service Packs".
- 2-10.2.1.3 A The *Initiate Payment 2* command shall be sent with empty amount fields.
- NOTE:** The empty amount fields will force the PSAM to send the *Get Amount 3* command in which the PAN is sent to the terminal.
- 2-10.2.1.4 A When the response to the *Initiate Payment 2* has been received, the *Set D/C Properties* command shall be sent including the additional transaction data, for further details see section 2-8.5.3 page 2-8-7. This command is defined in section 2-14.5.9 page 2-14-41.

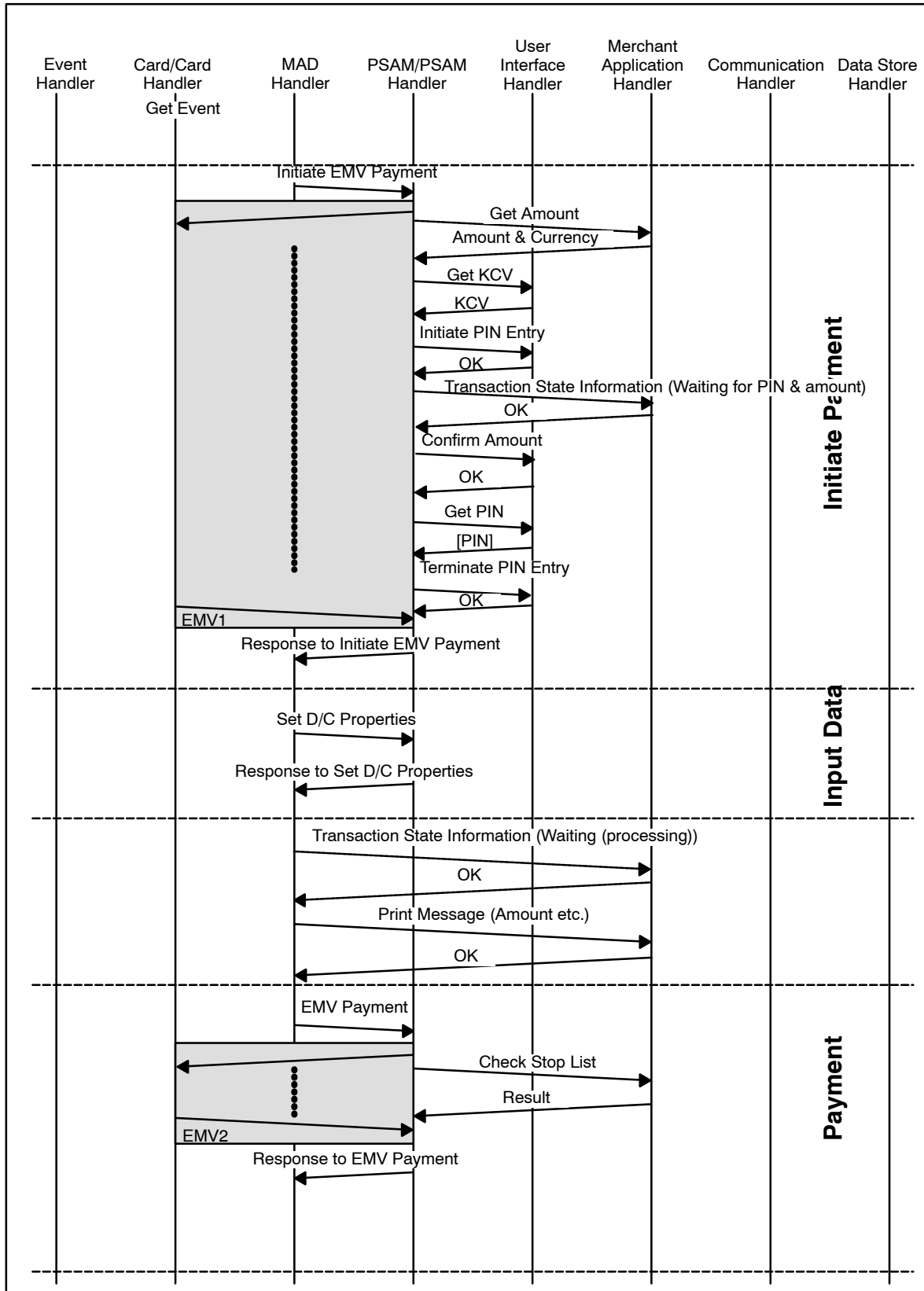


Figure 2-10.1 - General transaction flow

This page is intentionally left blank

2-11 Private Label Card Schemes

2-11.1 Handling of Private Label Cards

2-11.1.1 Introduction

This section specifies the flow when local magnetic stripe cards are handled in the terminal.

The actual dialog between the terminal and e.g. the Electronic Cash Register and how the Private Label Card scheme application is implemented are out of scope for this specification.

2-11.1.2 Description

Information on whether a particular card belongs to a Private Label Card scheme or not is obtained from track 2 of the magnetic stripe card and related parameters stored in the PSAM.

The Track 2 is forwarded to the PSAM by use of the *Get Debit/Credit Properties* command with Identifier = '0012'.

- 2-11.1.2.1 A A proprietary handling of a Private Label Card scheme application shall not be initiated, unless the PSAM in the response to the *Get Debit/Credit Properties* command indicates in the data element Card Service Info, that the Card (and PAN) is proprietary.

The coding of the data element Card Service Info can be found in section "Data Elements", subsection 2-15.2.31 (Card Service Info).

NOTE: Detection of whether or not a card belongs to a Private Label Card scheme is independent of whether or not the PSAM is able to perform a transaction using the card. I.e. a card from a Private Label Card scheme may be able to perform PSAM based transaction.

2-11.1.3 Flow

- 2-11.1.3.1 B The flow for a Private Label Card shall be as shown in figure 2-11.1.

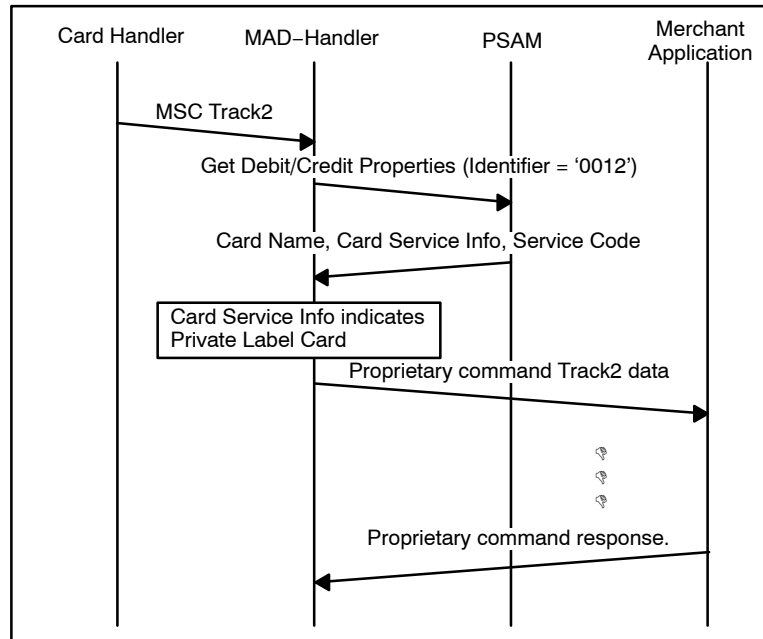


Figure 2-11.1 - Private Label Card Scheme message flow (Private Label Card)

If the PSAM indicates that the card in question is a *non* Private Label Card, the merchant can either choose to initiate a normal transaction using the PSAM or to interrupt the transaction in progress.

2-11.1.3.2

B The flow for a *non* Private Label Card shall be as shown in figure 2-11.2.

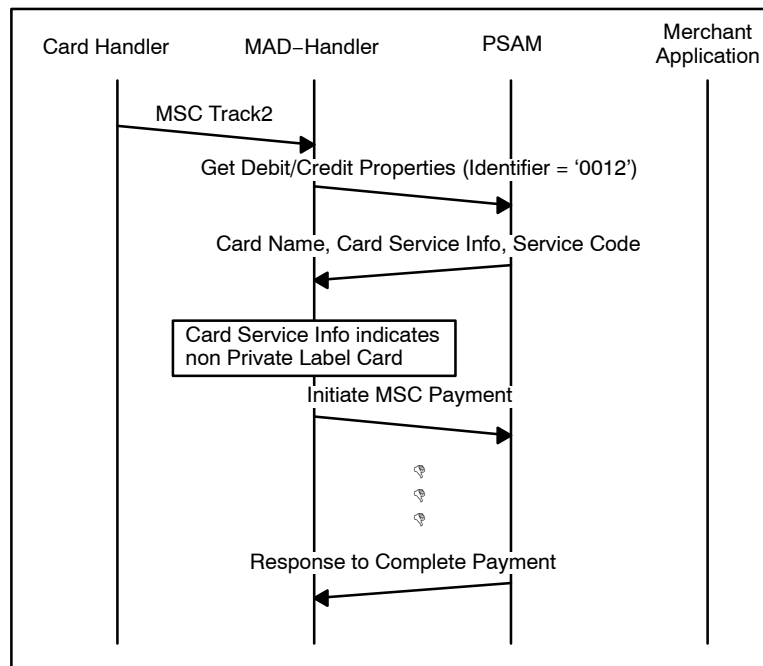


Figure 2-11.2 - Private Label Card Scheme message flow (Non Private Label Card)

2-12 Local PIN

2-12.1 Local PIN Validation Message Flow

2-12.1.1 Introduction

Local PIN is a functionality where a reference PIN is conveyed to the PSAM for comparison with the PIN entered on the PED by the cardholder. The PSAM will return the result of the comparison.

2-12.1.2 Description

The Local PIN Validation function shall be called from a separate application within the terminal, i.e. an application separate from the 'Nets debit/credit application'.

As Local PIN is handled by the PSAM for the Nets debit/credit application, the ID_{PSAMAPP} has to be '8111' when addressing the Nets PSAM.

The application using the Local PIN functionality shall make this conversion of ID_{PSAMAPP} when addressing the Nets PSAM. See example given in figure 2-12.1.

The application requesting Local PIN Validation shall send the request to the PSAM, and the PSAM will then interface to the PIN Entry Device, to process the requested function.

A single command, *Local PIN Validation*, sent to the PSAM includes the necessary information for performing a PIN entry sequence including amount acceptance if requested.

The messages displayed to the cardholder will be the same as used for PIN entry sequences for debit/credit transactions.

The response from the PSAM will never include the PIN entered, but only a result-code defining whether the PIN digits entered matched the one received from the application. The PIN entry may be cancelled/interrupted before completion.

Two methods for the transfer of the reference PIN is supported:

- The reference PIN is transferred in plaintext
- The reference PIN is transferred enciphered

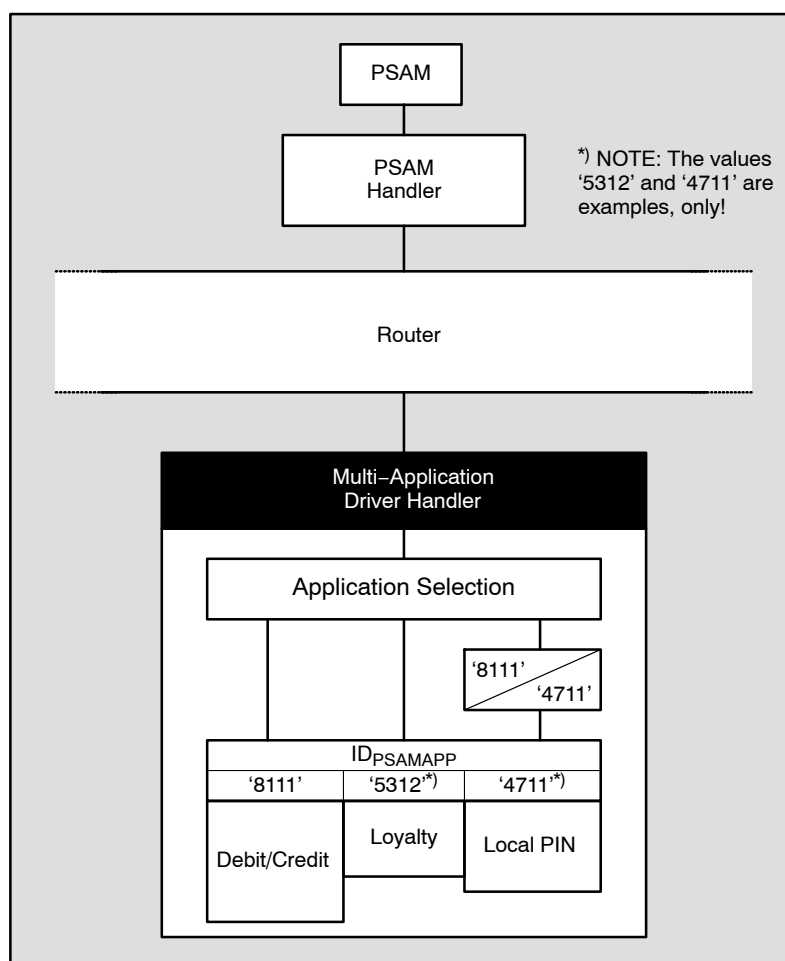


Figure 2-12.1 - TAPA Architecture

2-12.1.3 Local PIN Validation

Validation Flow

Figure 2-12.2 page 2-12-3 shows the validation flow for a successful Local PIN Validation. If the *Get KCV* command indicates that a synchronization of the PSAM/PIN Entry Device is required, the synchronization process known from the Debit/Credit application will be applied by the PSAM.

If the *Local PIN Validation* command contains the amount related fields, the Cardholder will be prompted to confirm the amount and PIN simultaneously.

The application may release the service/goods when a successful response to the *Local PIN Validation* command is received if other application specific conditions are fulfilled.

A final *Complete Payment* command is required to clean-up the PSAM.

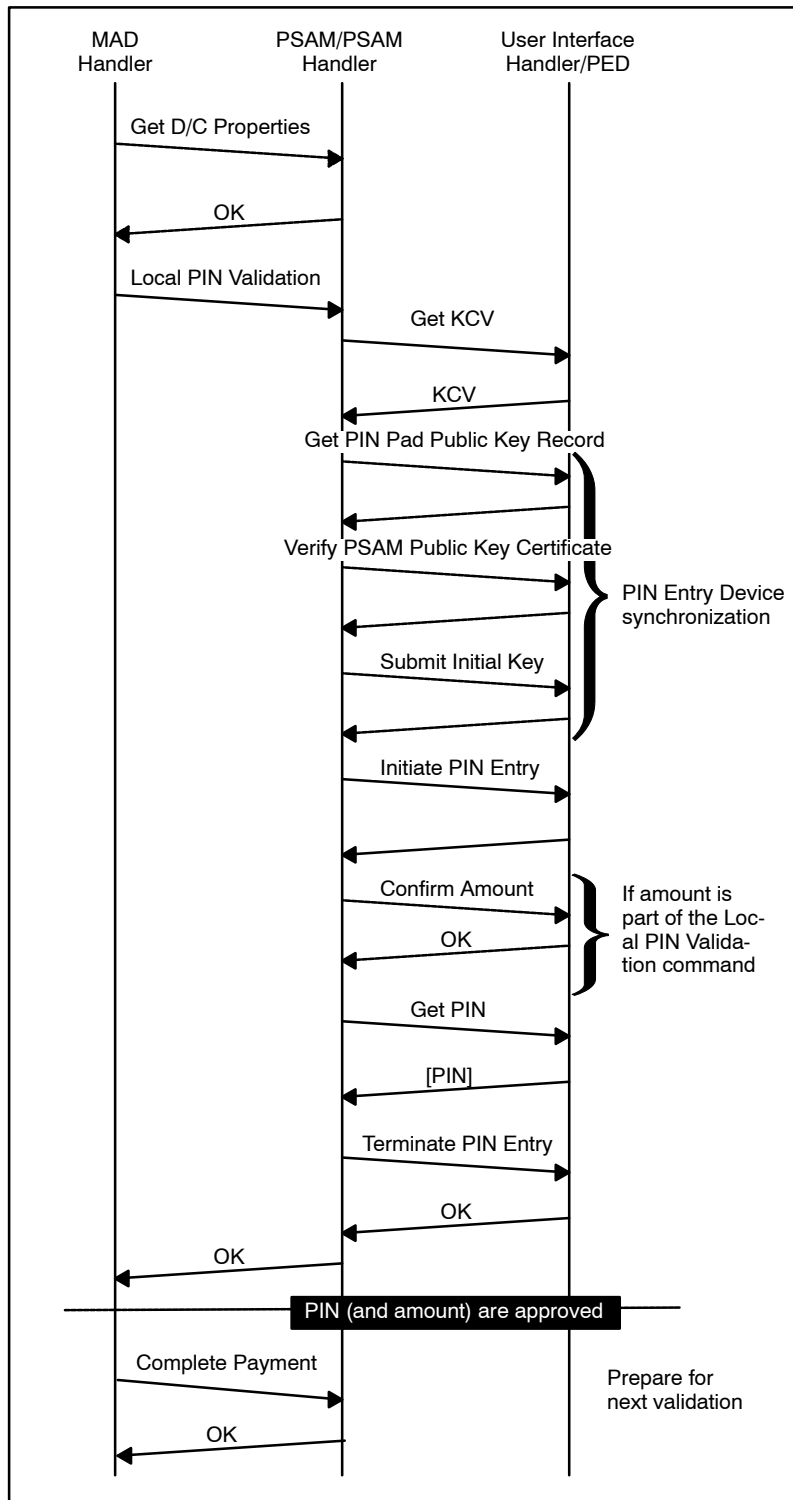


Figure 2-12.2 - Local PIN Validation Message Flow

NOTE: See also section 2-12.7 page 2-12-11 for an example of message flow.

2-12.2 Plaintext PIN Data

2-12.2.1 Local PIN Validation command - Plaintext PIN

When a plaintext PIN block is sent to the PSAM, the Method Number = '00' (plaintext PIN block) shall be used.

- 2-12.2.1.1 A The *Local PIN Validation* command sent to the PSAM shall have the format shown in table 2-14.133 page 2-14-124.

The response to *Local PIN Validation* command will have the format shown in table 2-14.134 page 2-14-125.

- 2-12.2.1.2 A The plaintext PIN block shall be formatted as described in figure 2-12.3.

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

where

	Name	Value
C	Control field	'02'
N	PIN length	4-bit binary number with permissible values of '4' to 'C'
P	PIN digit	4-bit field with permissible values of '0' to '9'
P/F	PIN/Filler	Determined by PIN length
F	Filler	4-bit binary number with value of 'F'

Figure 2-12.3 - Plaintext PIN Block

This PIN Block format is identical to the PIN block format defined in ref. 20: "EMV, version 4.2" for 'plaintext offline PIN block' in the *Verify* command.

2-12.3 Enciphered PIN Data

2-12.3.1 Key Management

Load of Keys

If the Local PIN Validation requires enciphered PIN, load of a key exchange key (LP-KEK) and a PIN protection key (LP-PPK) shall be initiated prior to performing PIN validation. The *Load LP Keys* command shall be issued at least twice, loading the the LP-KEK first followed by the LP PPK.

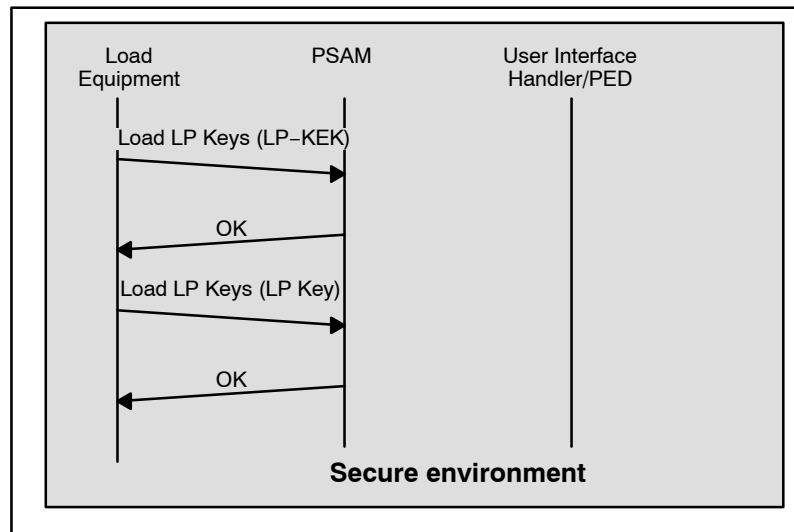


Figure 2-12.4 - Load LP Keys Message Flow

Structure

The PSAM is able to handle 4 key chains simultaneously. Depending on the actual implementation, the different chains may be assigned to different card schemes or may be used randomly by a single card scheme.

Each chain is identified by the data element LP-Key-Chain (values: '00' - '03').

Each chain consists of two key-levels.

On the upper level the LP-KEK contains the key used as master key for exchange of the lower level key LP-PPK. One LP-PPK is defined for each LP-KEK. See table 2-12.1 and 2-12.2.

LP-PPK is used to encipher the Enciphered PIN Data transferred to the PSAM in the *Local PIN Validation* command.

Table 2-12.1 - LP-Key-Chain - Upper Level

Key	Field	Value	Length
LP-KEK	LP-KEK-Version	Version of the actual LP-KEK-Data	1
	LP-KEK	Actual master key used for exchange of LP-PPK	16

Table 2-12.2 - LP-Key-Chain - Lower Level

Key	Field	Value	Length
LP-PPK	LP-PPK-Version	Version of the actual LP-PPK-Data	1
	LP-PPK	Actual key used for transfer of Enciphered PIN Data	16

With the capability of handling 4 key chains simultaneous, the complete data structure may be summarize by table 2-12.3.

Table 2-12.3 - LP-Key-Chain Structure

Key	Field	Length	LP-Key-Chain			
			'00'	'01'	'02'	'03'
LP-KEK	LP-KEK-Version	1				
	LP-KEK	16				
LP-PPK	LP-PPK-Version	1				
	LP-PPK	16				

The generation, distribution and maintenance of LP-KEK(s) and LP-PPK(s) are the responsibility of the owner(s) of the application using the *Local PIN Validation* command.

Only the commands used to exchange the keys in use are covered by this specification.

LP-KEK(s) should be loaded into the PSAM in a secure environment.

LP-PPK(s) may be loaded/substituted while the PSAM is under normal operation in a terminal.

It is not possible to read out neither the LP-KEK nor the LP-PPK from the PSAM.

The *Load LP Keys* command shall be used for loading the keys.

2-12.3.2 Load LP Keys Command

The *Load LP Keys* command shall be used for load/exchange of LP-KEK(s) and LP-PPK(s).

- 2-12.3.2.1 A The *Load LP Key* command sent to the PSAM shall have the format shown in table 2-14.131 page 2-14-122.

The Response to the *Load LP Key* command will have the format shown in table 2-14.132 page 2-14-123.

LP-KEK

When LP-KEK shall be exchanged the field LP-KEK-Data shall contain the new key value (LP-KEK_{NEW}) enciphered by the previous value of the same key:

LP-KEK-Data = DES3(LP-KEK _{PREVIOUS})[LP-KEK _{NEW}]

The initial value for the LP-KEK keys are a zero-key ('01 01 01...01 01').

LP-PPK

When LP-PPK shall be exchanged the field LP-KEK-Data shall contain the new key value (LP-PPK_{NEW}) enciphered by the corresponding LP-KEK key (within the same key-chain):

LP-PPK-Data = DES3(LP-KEK)[LP-PPK _{NEW}]

Key Check Value

The field Key Check Value shall contain the 3 most significant bytes of the result of a triple-DES encryption of an 8 byte

block of zeros (using the new LP-KEK or LP-PPK respectively):

Key Check Value =
 3MSB {DES3(LP-KEK_{NEW}) ['0000000000000000']}

or

Key Check Value =
 3MSB{DES3(LP-PPK_{NEW})['0000000000000000']}

The encryption performed on the data in the fields LP-KEK-Data and LP-PPK-Data shall follow the requirements for padding, triple DES and double length keys as defined in ref. 27: "TAPA Application Architecture version 2.1", section 14.6.4 and 14.6.5.

The Method Specific Response Data will be included in the responses irrespective of the value for Application Status Words.

NOTE: The only exception is when an invalid Method Number is presented (ASW1-ASW2 = '1F20'). A short response will be returned in this case.

The data elements defining the actual key versions may be needed to 'synchronize' the keys used by the PSAM with the keys used by the entity computing the Enciphered PIN Data.

2-12.3.3 Local PIN Validation command - Enciphered PIN

- 2-12.3.3.1 A When enciphered PIN is used, the *Local PIN Validation* command sent to the PSAM shall have the format shown in table 2-14.135.

A successful response to the *Local PIN Validation* command will have the format shown in table 2-14.137 page 2-14-127.

The data element LP-Key-Chain shall indicate the actual key-chain used to encipher the PIN data.

The different key-chains may be assigned to be used by individual card schemes. Other principles may be used, depending on the actual implementation.

The data element LP-PPK-Version shall indicate the version of the actual key, used to encipher the PIN data.

The data element Random Pad Pattern shall be included in the block of data to be enciphered.

The Random Pad Pattern will ensure that the resulting Enciphered PIN data block varies, even if the PIN is the same.

Encipherment

The encipherment performed on the data in the field Enciphered PIN Data shall follow the requirements for padding, triple DES and double length keys as defined in ref. 27: "TAPA Application Architecture, version 2.1", section 14.6.4 and 14.6.5.

Transaction Counter Validation

The Local PIN Validation functionality offers tools to reduce replay attacks when using enciphered PIN.

By conveying a Transaction Counter value in the the *Local PIN Validation* command, the PSAM will detect if any replay is attempted. If the value is less than or equal to the actual value maintained in the PSAM, the PIN validation will be rejected and the transaction counter will not be incremented. The initial value of the PSAM counter is zero. The PSAM holds a Transaction Counter for each key chain.

If the Transaction Counter value is higher than the actual value and the gap is less than 14, the PSAM counter will be incremented and PIN validation will proceed. If the gap is higher than 14, the PIN validation will be rejected and the transaction counter will not be incremented. See example in figure 2-12.5 page 2-12-9.

The allowed offset of 14 is designed to handle incorrect PIN entries without requiring a new (reference) PIN block from the entity generating the Enciphered PIN Block.

If the Transaction Counter value is set to zero, no Transaction Counter Validation will take place.

NOTE: Transaction Counter Validation is not possible for plaintext PIN validations.

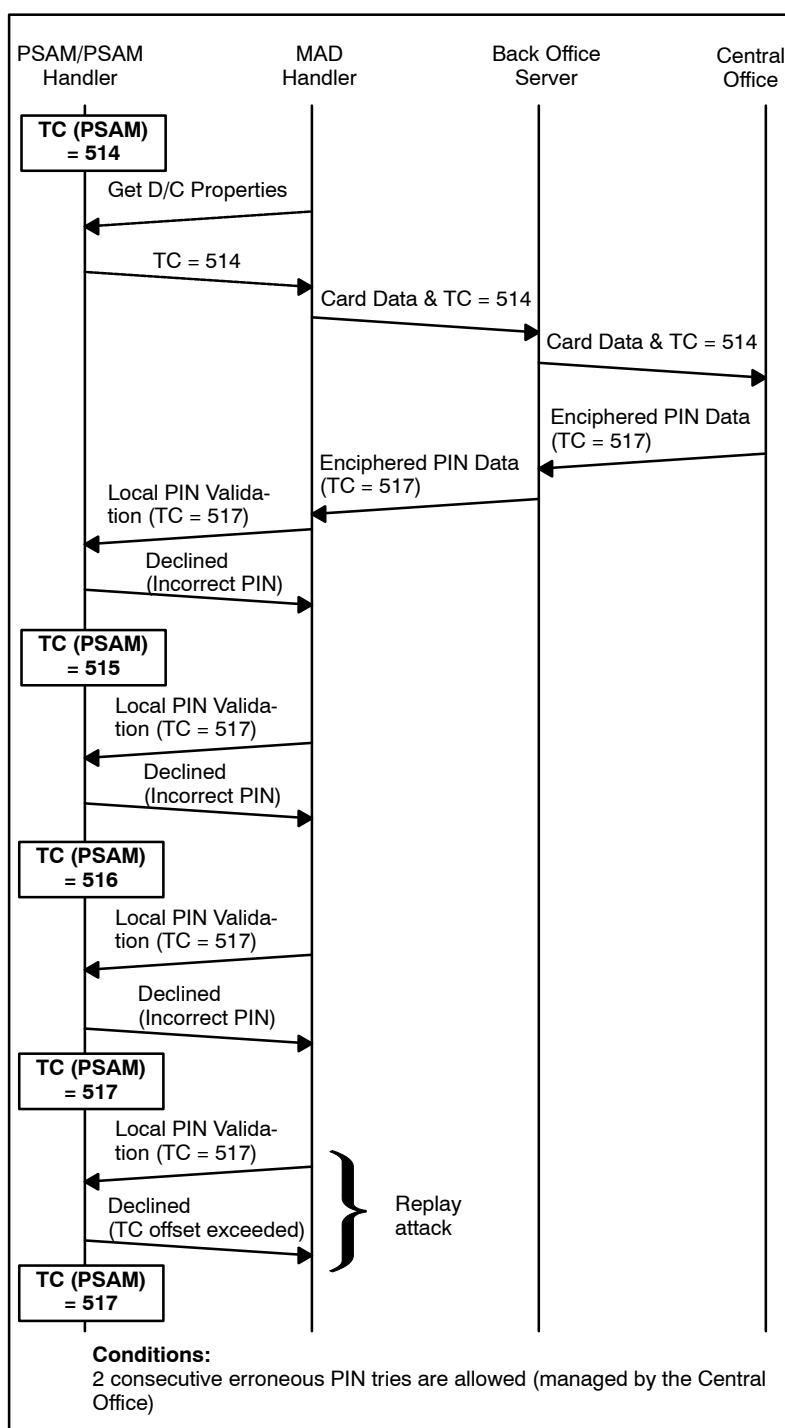


Figure 2-12.5 - Example of the Transaction Counter Handling

Transaction Counter Synchronization

Prior to issuing the *Local PIN Validation* command, the local PIN application may decide to issue a *Get Debit/Credit Properties* command in order to obtain the current value of the transaction counter. See section 2-12.3.4 page 2-12-10 for more details.

The data element Transaction Counter will indicate the actual transaction sequence number.

2-12.3.4 Get Debit/Credit Properties Command

The *Get Debit/Credit Properties* command with Identifier = '06' is utilized to retrieve the following data elements for each key-chain:

- Transaction Counter
- LP-KEK-Version
- LP-PPK-Version

The format of the *Get Debit/Credit Properties* command/response is in section 2-14.5.8 on page 2-14-29.

2-12.3.5 Complete Payment Command

A final *Complete Payment* command is required to clean-up the entry in the PSAM. If clean-up is not performed no further validations for this entry is possible.

The format of the *Complete Payment* command/response is given in section 2-14.6.4 on page 2-14-65.

2-12.4 Limitations

2-12.4.1 Enabling/Disabling of the Local PIN Validation functionality

Local PIN is only available when Nets Denmark has enabled the function.

NOTE: If the command *Local PIN Validation* is sent without the functionality being enabled, ASW1-ASW2 = '1F00' (Local PIN disabled) will be received.

2-12.4.2 Availability of the Local PIN Validation functionality

Local PIN is only available when the PSAM is *not* busy:

- The PSAM must be installed and the PSAM/PED synchronization must be completed
- The PSAM must be in the state "Ready for transaction"
- One Thread must be free

2-12.4.3 PIN Range

- 2-12.4.3.1 A The number of PIN digits shall be in the range 4 - 12.

2-12.4.4 PIN tries

The maximum number of consecutive PIN tries without requesting a new reference PIN from the host is 14. It is up to local PIN validation application to define the number of PIN tries (normally set to 3).

2-12.5 Application Status Words (ASW1-ASW2)

For Application Status Words related to the Local PIN Validation, special ranges has been reserved:

Table 2-12.4 - ASW1-ASW2 Ranges

Command	ASW1-ASW2 range
Local PIN Validation	'1F00' – '1F1F'
Load LP Keys	'1F20' – '1F2F'
Get Debit/Credit Properties	See debit/credit section (2-14.10.1)

Table 2-12.5 - ASW1-ASW2 - PIN Rejected

Command	ASW1-ASW2
Local PIN Validation (Plaintext)	'1F0F'
Local PIN Validation (Enciphered)	'1F16'

NOTE: The actual values can be found in table 2-14.159 page 2-14-184 to table 2-14.162 page 2-14-185.

2-12.6 Message Codes

It is up to application owner to define relevant Message Codes (related to the ASW1-ASW2) to be displayed at the Cardholder Display.

2-12.7 Example of Message Flow

This section is intended to be used as information only.

Please find below a description of the message flow shown in figure 2-12.6 page 2-12-12.

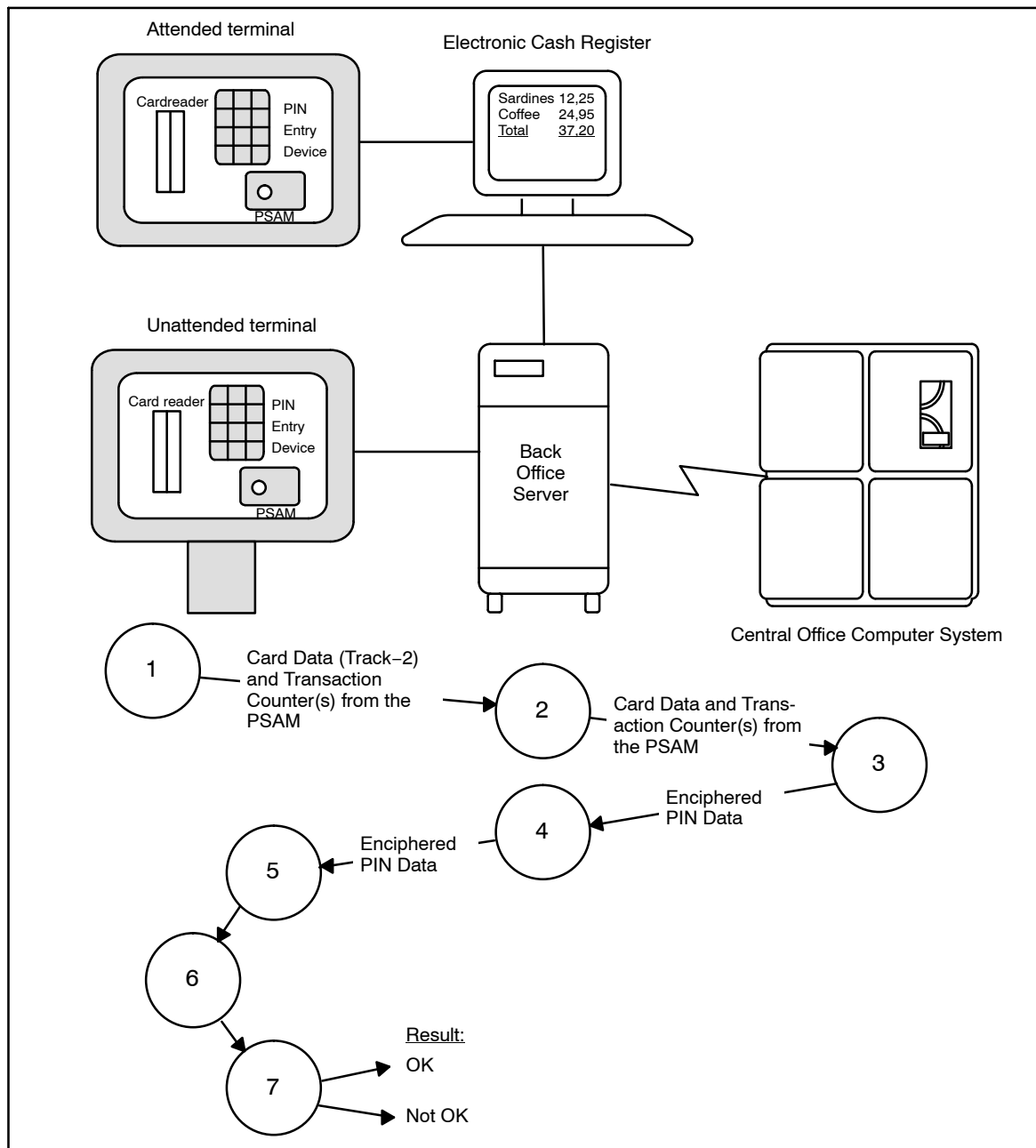


Figure 2-12.6 - Message Flow - Magnetic Stripe Cards

This description shall only be seen as an example of using Local PIN Validation. The description is based on a centralized system, where the calculation/look up for the PIN is processed in a Central Office Computer System, and the PIN is transmitted to the PSAM on encrypted form.

1. The card is inserted/swiped in the terminal, and the terminal equipment reads the Card Data, e.g. by reading Track-2 from the magnetic stripe. The actual value(s) of the Transaction Counters are retrieved from the PSAM. Card Data and Transaction Counter(s) are transmitted from the terminal equipment to the Back Office Server.
2. Card Data and counters are passed on from the Back Office Server to the Central Office Computer System.
3. Based on the Card Data received, the central system processes the request and generates a response, includ-

ing the PIN to be entered.

Based on the Transaction Counter value from the PSAM and the number of PIN tries left, the Central Office Computer System computes the value for the Transaction Counter in the Enciphered PIN Data.

To keep the PIN confidential, the PIN is transmitted as encrypted data.

4. The Back Office Server forwards the response to the terminal equipment.

5. The terminal equipment generates a request to the PSAM, for Local PIN Validation.

The request contains the PIN information received. The PIN information is transmitted on encrypted form, as it was calculated in the central system.

The PSAM unpacks the request for Local PIN Validation and sends to the PIN-pad a request for initiating PIN entry. The request to start the PIN entry is based on the same commands and same level of security, as all other requests for PIN entry.

6. The cardholder keys in the PIN and completes the PIN entry.

The PIN is transmitted to the PSAM.

The transfer of the PIN is based on the same commands and same level of security, as all other PINs transfers, from the PIN-pad to the PSAM.

7. The PSAM compares the PIN key-entered with PIN information received in the request for Local PIN Validation.

If the key-entered PIN is equal to the expected value, the PSAM will respond to the terminal equipment indication:

- Successful (ASW1-ASW2 = '0000').

If not, the response from the PSAM will indicate:

- Declined (ASW1-ASW2 = '1F0F' (Plaintext) or '1F16' (Enciphered) respectively).

The use of Local PIN Validation may be implemented in both attended and unattended (self service) terminals.

The figure shown on the previous page is based on Card Data read from the magnetic stripe of the card. The message flow does not depend on the card technology used. A similar message flow may be implemented using IC cards.

This page is intentionally left blank

2-13 Host Communication for the Debit/Credit Application - Protocols and Formats

2-13.1 Introduction

This section defines the communication with the Terminal Operator host when performing debit/credit transactions.

The message formats are based on ref. 25: "APACS Standard 60".

The notation used in this section is defined in section 1-4.2.3 page 1-4-5.

2-13.2 General

In this section, the term transaction is defined as series of data transmissions from the terminal to the Terminal Operator and back, i.e. a transaction is a full job.

Whenever a transaction is ended, the session shall be terminated. A repetition shall establish a new session.

When all sessions have been terminated, the physical link (carrier) will be disconnected by the Terminal Operator.

Primary and Secondary Access Points

To ensure the highest level of accessibility to the Nets Denmark A/S platforms for online authorization and advice transfer, dual access points are established for the involved platforms.

The device making the connection to Nets Denmark A/S (the CAD or terminal server depending on the network topology) is responsible for using both the primary and secondary access point.

2-13.3 Communication Protocols

In order to be able to communicate with the Terminal Operator, a communication protocol is needed.

The communication protocol stack is defined as shown in table 2-13.1.

Table 2-13.1 - Protocol Layers

Layer	Name	Implementation	Remarks
7	Application layer	APACS60	Includes additional Header
6	Presentation layer		
5	Session layer		
4	Transport layer	TCP	
3	Network layer	IP	
2	Data link layer	PPP	Without PAP or CHAP
1	Physical layer	PSTN	All V. standards except V.90
		ISDN	V.120 without LLC
		ISDN	“Raw” ISDN
		ISDN	HDLC/X.75
		GSM	V.110
		VPN/LAN	ADSL, GPRS, ...

2-13.3.1 Physical Layer

- 2-13.3.1.1 B The physical layer may either be a switched network (e.g. PSTN, ISDN or GSM) or a (virtual) permanent network (e.g. GPRS, ADSL or VPN).
- 2-13.3.1.2 A The terminal shall be able to support two access points on the host platforms. Each access point identified by individual addresses (dial-up, IP- and Port- numbers).
- 2-13.3.1.3 A It shall be possible to update both set of address parameters.
- 2-13.3.1.4 A If a switched/Dial-up network is used (PSTN, ISDN or GSM) the terminal shall be connected to a line where the A-number is transferred to the Nets Denmark A/S platform.

NOTE: When the network transfers the A-number to the Nets Denmark A/S platform, the host systems will be able to identify the terminals address on the network.

2-13.3.2 Data Link Layer

- 2-13.3.2.1 A The data link layer shall use PPP on switched/Dial-up lines.
The assigned IP addresses will be without authenticity and consequently there is no use of neither PAP nor CHAP.

2-13.3.3 Network Layer

- 2-13.3.3.1 A The network layer shall be Internet Protocol (IP).
The access server or dial-in router will contain a range of IP addresses which will be assigned dynamically.

2-13.3.4 Transport Layer

- 2-13.3.4.1 A Each terminal entity (CAD) shall use a unique TCP address (port number). This entity must establish a session with a corresponding TCP entity at the Terminal Operator.
- 2-13.3.4.2 C Mapping of the terminal entity to the TCP address may be performed either in software or in a router.

2-13.3.5 Session Layer

The session layer carries the authorization transactions, the financial notifications, etc.

2-13.3.6 Presentation and Application Layers

The presentation and application layers are specified in the remaining part of this section.

- 2-13.3.6.1 A The communication interface shall be able to send and receive messages of a size up to at least 1K bytes.

2-13.4 Transmission Flows

The transmission flows for the different debit/credit transaction types are described in chapter 2-5 page 2-5-1, Debit/Credit Functionality.

2-13.5 Transmission Formats

2-13.5.1 APACS Message Types

Table 2-13.2 lists the APACS message types used in the OTRS environment.

Table 2-13.2 - APACS Message Types used in OTRS

ISO	MTI	Message Type	Source	Transaction Type/Process
1100	0106	Authorization Request	PSAM	Original/Extended Authorization Supplementary Authorization Purchase online (EMV)
1101	0107	Authorization Request Repeat	PSAM/CAD	
1110	0116	Authorization Request Response	Host	
1120	0126	Authorization Advice	PSAM	Original/Extended Authorization (rejected) Supplementary Authorization (re- jected) Purchase (EMV) (rejected) Refund (rejected)
1121	0127	Authorization Advice Repeat	PSAM/CAD	
1130	0136	Authorization Advice Response	Host	
1200	0206	Financial Request	PSAM	Purchase online (MSC + Key Entered) Refund online
1201	0207	Financial Request Repeat	PSAM/CAD	
1210	0216	Financial Request Response	Host	
1220	0226	Financial Advice	PSAM	Capture Purchase offline Purchase online (EMV) Offline Refund
1221	0227	Financial Advice Repeat	PSAM/CAD	
1230	0236	Financial Advice Response	Host	
-	0360	File Action Instruction	Host	PSAM Update Transfer
-	0364	File Action Instruction	Host	Consolidated Reconciliation
1304	0370	File Action Instruction Ack.	CAD	PSAM Update Transfer
-	0374	File Action Instruction Ack.	CAD	Consolidated Reconciliation
1420	0426	Reversal Advice	PSAM	Reversal (Authorization) Purchase (failed) Refund (failed) Original/Extended Authorization (failed) Supplementary Authorization (failed)
1421	0427	Reversal Advice Repeat	PSAM/CAD	
1430	0436	Reversal Advice Response	Host	
1304	0624	Administrative Advice	PSAM	Addendum Records Service Records
1305	0625	Administrative Advice Repeat	PSAM/CAD	
1314	0634	Administrative Advice Response	Host	
-	0804	Network Management Request	PSAM/CAD	Installation Advice Transfer PSAM Update PSAM Deactivation Clock Synchronization Generate Reconciliation Reconciliation Report
-	0805	Network Management Request Repeat	CAD	
-	0814	Network Management Request Response	Host	
-	0844	Network Management Notification	CAD/Host	

2-13.5.2 APACS Message Header

Purpose

In order to ease message routing and format recognition and because host messages generated by the PSAM are enciphered, a message header precedes the actual APACS 60 messages.

Depending on the message type, different fields are required in the APACS Message Header.

TLV-coding for the APACS Message Header

The APACS Message Header consists of a number of fields. The first two fields (protocol type and protocol version) have fixed formats, whereas the following fields are TLV-coded. This allows fields to be present or not depending on the actual situation. Furthermore, new fields may be introduced in later versions without affecting current implementations as unknown/unsupported fields may be ignored.

Structure of the Tag Field

The tag field of a TLV-structure consists of one or two bytes. The coding of these bytes shall be consistent with the basic encoding rules (BER-TLV) of ASN.1. Table 2-13.3 defines the first byte.

NOTE: Multiple occurrences of a data object shall not appear.

Table 2-13.3 - Structure of the first Byte of a Tag

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	–	–	–	–	–	–	<u>Tag class:</u>
0	0	–	–	–	–	–	–	Universal (not used in this specification)
0	1	–	–	–	–	–	–	Application-specific (not used in this specification)
1	0	–	–	–	–	–	–	Context-specific (not used in this specification)
1	1	–	–	–	–	–	–	Private (defined in this specification)
–	–	x	–	–	–	–	–	<u>Tag type:</u>
–	–	0	–	–	–	–	–	Primitive Data Object
–	–	1	–	–	–	–	–	Constructed Data Objects
–	–	–	x	x	x	x	x	<u>Tag value:</u>
–	–	–	X	X	X	X	X	The Tag is 1 byte long. The value, in the range 0..30, is contained in b1–b5
–	–	–	1	1	1	1	1	The Tag is 2 bytes long. The value, in the range 31..127, is contained in the second byte

- 2-13.5.2.1 A The coding of the second byte, when present, shall be:
b8=0
b7 to b1=binary value of the Tag number in the range 31..127.

Table 2-13.4 lists the data objects presently defined.

The APACS Header itself (tag='E0') is a Constructed Data Object, i.e. the value field is a concatenation of zero or more Data Objects. These Data Objects themselves may be Primitive and/or Constructed.

Table 2-13.4 - List of Data Objects for use in the APACS Header

Tag	Attrib.	Length	Comment
'C0'	b2	2	Length of the following ¹⁾ APACS 60 message
'C1'	an4	4	Message Type Identifier
'C2'	n3	2	Function Code (identical to field 24)
'C3'	b13	13	PSAM Identifier (identical to field 60, exclusive the length field)
'C4'	n6	3	Systems Trace Audit Number (identical to field 11 if this is present)
'C5'	b1	1	KEK _{DATA} version (key version for key using to encipher KSES _{DATA})
'C6'	b16	16	[KSES _{DATA}] (enciphered key for APACS 60 message)
'C7'	b1	1	APACS MAC Key version
'C8'	n3	2	Advice Window Size
'C9'	b1	1	PSAM Update Flag
'CA'	..anps20	..20	Display line for host error message
'CB'	b1	1	Network Connection Type
'CC'	ans8	8	MAD-Handler ID
'CD'	an8	8	Terminal Identification
'CE'	..b8	..8	Proprietary Data (echoed by the host)
'CF'	b21	21	Communication interface statistics
'D1'	n6	3	Reference STAN
'D2'	an4	4	MTI of the original message (0206 or 0226)
'E0'	-	var.	APACS 60 header type 0
'E2'	-	var.	Host error message

Notes: ¹⁾ The Length field ('C0') may not be the last field in the APACS Header

NOTE: Tags for communication error counters and statistical data are to be defined.

Coding of the Length Field

The length field of a TLV-structure is coded according to a subset of the ASN.1 rules.

- 2-13.5.2.2 A Depending on the value of L its length may be 1, 2 or 3 bytes as defined in table 2-13.5. The shortest possible form shall always be selected.

Table 2-13.5 - Coding of the Length Field

Range	No. of bytes	1st byte	2nd byte	3rd byte
0..127	1	Binary value		
128..255	2	'81'	Binary value	
256..65535	3	'82'	Binary value	

Coding of the Value Field

The coding of the value field of a TLV-structure depends on the actual data element. Value fields for Primitive Data Objects are defined in section 2-13.7 page 2-13-14.

General APACS Message with Header

Table 2-13.6 defines the general format for an APACS Message including the APACS Header.

Table 2-13.6 - General APACS Message with Header

Field name	Attrib.	Length	Value
Protocol type	an3	3	"A60" (APACS 60)
Protocol version	an1	1	"1" for this version
APACS Header, type 0	–	var.	Constructed Data Object, Tag='E0'
APACS message	–	var.	See table 2–13.14 and forward

APACS Header Generated by the PSAM

Request and advice messages created by the PSAM are always MAC'ed and enciphered to protect them during transmission over open networks.

Consequently, information on the encipherment keys involved are included in the APACS Header (also generated by the PSAM).

- 2-13.5.2.3 A All data objects in the APACS Header generated by the PSAM shall be transmitted by the CAD.

NOTE: The PSAM will include all mandatory data objects defined in table 2-13.7.

Table 2-13.7 - PSAM Generated Data Objects in the APACS Header

MTI	Tag												
	'C0'	'C1'	'C2'	'C3'	'C4'	'C5'	'C6'	'C7'	'CC'	'CD'	'D1'	'D2'	'E0'
0106	M	M	M	M	M	M	M	M	M	M	-	-	M
0107	M	M	M	M	M	M	M	M	M	M	-	-	M
0126	M	M	M	M	M	M	M	M	M	M	-	-	M
0127	M	M	M	M	M	M	M	M	M	M	-	-	M
0206	M	M	M	M	M	M	M	M	M	M	-	-	M
0207	M	M	M	M	M	M	M	M	M	M	-	-	M
0226	M	M	M	M	M	M	M	M	M	M	M	M	M
0227	M	M	M	M	M	M	M	M	M	M	M	M	M
0426	M	M	M	M	M	M	M	M	M	M	C2	C2	M
0427	M	M	M	M	M	M	M	M	M	M	C2	C2	M
0624	M	M	M	M	M	M	M	M	M	C1	-	-	M
0625	M	M	M	M	M	M	M	M	M	C1	-	-	M
0804	M	M	M	M	-	-	-	C1	M	-	-	-	M
0805	M	M	M	M	-	-	-	C1	M	-	-	-	M

Legend:
C1: Conditional (present if the corresponding field is present in the message)
C2: Conditional (present if the Reversal has financial impact, i.e. the original MTI is either 0206 or 0226).
M: Mandatory
O: Optional
N/A: Not Applicable
-: Not Present

- 2-13.5.2.4 C The CAD may add further data objects to the APACS Header generated by the PSAM before sending the entire message. In this case, care shall be taken to adjust the length field for the header itself (tag='E0').

APACS Header Extended by the CAD

Even though the APACS Header is generated by the PSAM for most messages, the CAD or terminal server must fill in supplementary information related to communication.

- 2-13.5.2.5 A The CAD shall add the data object Network Connection Type (Tag 'CB') in the APACS Header if the value is '00', see definition in section 2-13.7.12 page 2-13-15.
- 2-13.5.2.6 A The terminal server shall add the data object Network Connection Type (Tag 'CB') in the APACS Header if the value is 01 or 02, see definition in section 2-13.7.12 page 2-13-15.
- The data object Communication Interface Statistics (Tag 'CF') shall be inserted in the APACS header by the communication interface to inform the host about the quality of the connection between the communication interface and Nets Denmark A/S.
- 2-13.5.2.7 A The Communication Interface Statistics shall be included in the header of the next APACS transaction if one of the following cases occur:

- Connection Errors different from zero
- Connection Request is greater than 99

NOTE: See table 2-13.13 page 2-13-18 for the definition of the data elements.

NOTE: The communication interface is the interface responsible for the TCP/IP communication with Nets Denmark A/S according to Tag 'CB' (Network Connection Type).

NOTE: Requirement 2-13.5.2.7 is also applicable for APACS headers generated by the CAD.

APACS Header Generated by the CAD

Request and advice messages created by the CAD (usually the MAD-Handler) are not enciphered but in order to facilitate easy message recognition and routing, an APACS Header is added.

- 2-13.5.2.8 A The CAD shall include all mandatory data objects defined in table 2-13.8 page 2-13-9 in the APACS Header when sending a self-generated message to the host.

Table 2-13.8 - CAD Generated Data Objects in the APACS Header

MTI	Tag								
	'C0'	'C1'	'C2'	'C3'	'CB'	'CC'	'CE'	'CF'	'E0'
0370	M	M	–	M	M	M	O	O	M
0374	M	M	M	M	O	M	O	O	M
0804	M	M	M	C	M	M	O	O	M
0805	M	M	M	C	M	M	O	O	M
0844	M	M	M	C	–	M	O	O	M

Legend:
C: Conditional (present if the corresponding field is present in the message)
M: Mandatory
O: Optional
N/A: Not Applicable
–: Not Present

APACS Header Generated by the Host

Request and advice messages created by the host are not enciphered but in order to facilitate easy message recognition and routing and to provide control information to the CAD itself, an APACS Header is added.

- 2-13.5.2.9 A The APACS Header shall be discarded by the CAD for messages forwarded to the PSAM.

The data objects marked as M (mandatory) in table 2-13.9 will be included in the APACS Header sent by the host.

- 2-13.5.2.10 A If a data object is unknown to the CAD or if it cannot be handled in the actual situation, it shall be ignored (i.e. the APACS Header shall not be rejected due to such circumstance).

Table 2-13.9 - Host Generated Data Objects in the APACS Header

MTI	Tag															
	'C0'	'C1'	'C2'	'C3'	'C4'	'C8'	'C9'	'CA'	'CC'	'CD'	'CE'	'CF'	'D1'	'D2'	'E0'	'E2'
0116	M	M	-	M	M	O	O	O	M	M	E	E	-	-	M	O
0136	M	M	-	M	M	O	-	O	M	M	E	E	-	-	M	O
0216	M	M	-	M	M	O	O	O	M	M	E	E	-	-	M	O
0236	M	M	-	M	M	O	-	O	M	M	E	E	O	O	M	O
0360	M	M	M	M	-	O	-	-	M	-	E	E	-	-	M	-
0364	M	M	M	M	-	O	-	-	M	M	E	E	-	-	M	-
0436	M	M	-	M	M	O	-	O	M	M	E	E	O	O	M	O
0634	M	M	-	M	M	O	-	O	M	C	E	E	-	-	M	O
0814	M	M	-	C	-	O	-	O	M	-	E	E	-	-	M	O
0844	M	M	M	-	-	O	-	-	M	-	E	E	-	-	M	-

Legend:
C: Conditional (present if the corresponding field is present in the message)
E: Echoed if present in message from the terminal
M: Mandatory
O: Optional
N/A: Not Applicable
-: Not Present

Example of an APACS Message with Header

An example of an APACS message, as transmitted, is given in table 2-13.10.

Table 2-13.10 - Example of an APACS Message with Header

Field name	Tag	Attrib.	Length	Value (hex) including Tag, Length
Protocol type	–	an3	3	41 36 30 (“A60”)
Protocol version	–	an1	1	31 (“1”)
APACS Header, type 0	‘E0’	–	var.	E0 5B (Header length = 91)
Length of APACS msg.	‘C0’	b2	2	C0 02 00 E6 (Length = 230)
Message Type Identifier	‘C1’	an4	4	C1 04 30 31 30 36 (MTI=“0106”)
APACS MAC Key Version	‘C7’	b1	1	C7 01 0A (Key# 10)
KEK _{DATA} Version	‘C5’	b1	1	C5 01 04 (Key# 4)
[KSES _{DATA}]	‘C6’	b16	16	C6 10 94 74 5D EA 75 4F 01 AB 76 9A 33 CA 67 3A DF 8B (enciphered key)
Function Code	‘C2’	n4	2	C2 02 01 01 (101: Original/Extended authorization, estimated amount)
Terminal Identification	‘CD’	an8	8	CD 08 54 45 52 4D 30 30 30 39 (“TERM0009”)
STAN	‘C4’	n6	3	C4 03 01 79 64 (STAN = 17964)
MAD–Handler ID	‘CC’	ans8	8	CC 08 31 32 33 34 35 36 37 38 (= “12345678”)
Communication Interface Statistics	‘CF’	–	var.	CF 08 12 34 56 78 9A BC DE F0 ¹⁾
PSAM Identifier	‘C3’	b13	13	C3 0D A0 00 00 01 20 00 00 00 05 03 95 6A 56 RID _{PSAM} = ‘A000000120’ (PBS Data) ID _{PSAMCREATOR} = 5 ID _{PSAM} = 60123734 (‘03956A56’)
Network Connection Type	‘CB’	b1	1	CB 01 00 (0: Terminal directly connecting to PBS)
APACS message	–	–	–	92 8A 65 82 ... (arbitrary example showing an enciphered message) This examples assumes a total length of 230 bytes for the enciphered APACS message.
NOTE: ¹⁾ The length of 8 bytes is just an example.				

2-13.6 Communication Statistics and Error Counters

2-13.6.1 Introduction

Certain errors are counted to enable the Terminal Operator to perform central surveillance of the terminals. In the same way, certain communication interface statistics, including response times, are collected by the terminal and transmitted to the Terminal Operator.

2-13.6.2 Communication Interface Statistics

Depending on the nature and source of data elements for communication statistical information, are *either* placed in the APACS Header *or* in field 46 (CAD Management/Service Quality Data) of the APACS Message.

Data that relates to the physical transmission line are placed in the APACS Header as this point may be remote from a PSAM and may serve more than one terminal/PSAM.

Data that relates to the experience as seen by the cardholder and merchant are placed in field 46. This requires access to the PSAM generating the APACS Message as this is MAC'ed and enciphered.

2-13.6.3 Error Counters

Depending on their nature and source, error counters may be reported in *either* the APACS Header *or* in field 46 (CAD Management/Service Quality Data) of the APACS Message.

Error counters related to the experience as seen by the cardholder and merchant are placed in field 46 (requiring the data to be transmitted to the PSAM at transaction time).

- 2-13.6.3.1 A The terminal shall have error counters for (at least) the following errors, see table 2-13.11:
- No response from Nets Denmark A/S (no of time-outs)
 - Card Reader error (Magnetic stripe and ICC)
 - Unsupported cards
 - Communication errors between the CAD and the Merchant Application
- 2-13.6.3.2 A The terminal or terminal server shall have error counters for (at least) the following errors:
- Communication errors related to a public network, see table 2-13.13 page 2-13-18.

Table 2-13.11 - Communication Interface Statistics and Error Counters

	Communication Interface Statistics	Error Counters
APACS Header	Communication interface statistics related to a public network	Communication errors related to a public network
Field 46	Response time for previous online transaction	No response from Nets Denmark A/S (number of time-outs) Card reader errors Unsupported cards Communication errors with the Merchant Application

2-13.6.4 Error Counters, tag TE, TF, TG and TH

The four Error Counters controlled and incremented by the terminal is conveyed to the PSAM in *Initiate Payment* command.

The requirements and guidelines, defining the situations in which the individual Error Counter shall be incremented, are described in this section.

Tag 'TE' - Number of time-outs

- 2-13.6.4.1 A The counter for tag 'TE' shall be incremented every time an APACS message have been sent but no response have been received.

NOTE: Request- , Advice- and Administrative- messages shall cause that the error counter is incremented.

Tag 'TF' - Number of Card Reader Errors

- 2-13.6.4.2 A When reading a MSC, the counter for tag 'TF' shall be incremented when the conditions in requirement 2-4.7.2.10 page 2-4-8 have been fulfilled.

- 2-13.6.4.3 A When reading an ICC, the counter for tag 'TF' shall be incremented when the sub-handler ICCR detects an error.

NOTE: Data element errors shall not result in incrementation of the counter.

Tag 'TG' - Unsupported Cards

- 2-13.6.4.4 A When reading a MSC, the counter for tag 'TG' shall be incremented when the conditions in requirement 1-14.3.4.5 page 1-14-12 have been fulfilled.

- 2-13.6.4.5 A When reading an ICC, the counter for 'TG' shall be incremented when:

- Application selection did not complete successful i.e. Initiate EMV Payment was not sent to the PSAM and
- the transaction was not cancelled by either the cardholder nor the merchant and
- the counter for tag 'TF' have not been incremented in the current payment session.

NOTE: Tag 'TG' does include technical reasons which results in the terminal not being able to successfully complete application selection, e.g. error in tags used during application selection.

Tag 'TH' - Communication errors between the CAD and the Merchant

- 2-13.6.4.6 A The counter for 'TH' shall be incremented when errors, which have not been surmounted, between the terminal (cardholder interface) and the merchants part of the terminal (merchant interface) have been detected.

2-13.7 Primitive Data Objects for the APACS Header

This subsection defines the coding of primitive data objects for use in the APACS Header.

2-13.7.1 Coding of Tag 'C0' (Length of APACS 60 Message)

- 2-13.7.1.1 A The value field for Tag 'C0' shall be coded on two bytes binary.

2-13.7.2 Coding of Tag 'C1' (Message Type Identifier)

- 2-13.7.2.1 A The value field for Tag 'C1' shall be coded on 4 bytes as 4 digits using the character set defined in ref. 12: "ISO/IEC 8859-15".

2-13.7.3 Coding of Tag 'C2' (Function Code)

- 2-13.7.3.1 A The value field for Tag 'C2' shall be coded as defined in section 2-13.9.6 page 2-13-79.

2-13.7.4 Coding of Tag 'C3' (PSAM Identifier)

- 2-13.7.4.1 A The value field for Tag 'C3' shall be coded as defined in section 2-13.9.16 (without the length field required when transmitted in field 60).

2-13.7.5 Coding of Tag 'C4' (Systems Trace Audit Number)

When Tag 'C4' is inserted by the PSAM, the value field will be coded on 3 bytes as 6 BCD digits. The value will be different for all transactions generated by the PSAM as it is based on an internal counter.

When Tag 'C4' is inserted by the host, the value field will be echoed as received in the incoming transaction.

2-13.7.6 Coding of Tag 'C5' (KEK_{DATA})

- 2-13.7.6.1 A This data object (Tag 'C5') shall never be inserted by the CAD.

2-13.7.7 Coding of Tag 'C6' ([KSES_{DATA}])

- 2-13.7.7.1 A This data object (Tag 'C6') shall never be inserted by the CAD.

2-13.7.8 Coding of Tag 'C7' (APACS MAC Key Version)

- 2-13.7.8.1 A This data object (Tag 'C7') shall never be inserted by the CAD.

2-13.7.9 Coding of Tag 'C8' (Advice Window Size)

- 2-13.7.9.1 A This data object (Tag 'C8') shall never be inserted by the CAD.
- 2-13.7.9.2 A When Tag 'C8' is received from the host, the value field shall be interpreted as 3 BCD digits coded on two bytes.

2-13.7.10 Coding of Tag 'C9' (PSAM Update Flag)

- 2-13.7.10.1 A This data object (Tag 'C9') shall never be inserted by the CAD.
- 2-13.7.10.2 A When Tag 'C9' is received from the host, the value field shall be interpreted as a boolean coded on the least significant bit of a single byte. The remaining bits are RFU and will initially be set to zero. Their value shall, however, be ignored by the CAD.

Consequently, the following values are presently defined:

'00': No specific request.

'01': The CAD is requested to perform a PSAM Update.

- 2-13.7.10.3 A When Tag 'C9' is received and the value indicates that PSAM Update is to be performed, a message shall be displayed on the Merchant Display in at least 6 seconds or until the merchant manually confirm the message.

NOTE: If the CAD automatically initiates an PSAM update sequence, no message needs to be displayed.

2-13.7.11 Coding of Tag 'CA' (Display Line for Host Message)

- 2-13.7.11.1 A This data object (Tag 'CA') shall never be inserted by the CAD.
- 2-13.7.11.2 A When Tag 'CA' is received by the CAD, it shall be interpreted as a text string for display purposes, e.g. in case the front-end at the Terminal Operator is functioning but no connection to the host system can be made. The display line is coded using the character set defined in ref. 12: "ISO/IEC 8859-15". The length is variable up to 20 bytes.
- 2-13.7.11.3 A When Tag 'CA' is received the text included shall be displayed on the Merchant Display in at least 6 seconds or until the merchant manually confirms the message.

NOTE: If Tag 'CA' is received more than once during a communication sequence, only the first reception needs to initiate the message to be displayed.

2-13.7.12 Coding of Tag 'CB' (Network Connection Type)

- 2-13.7.12.1 A The value field for Tag 'CB' shall inform the host of the network topography used for the particular transaction. One of the values defined in table 2-13.12 shall be used.

Table 2-13.12 - Coding of the Network Connection Type

Value	Meaning
'00'	The transaction is generated in a stand-alone terminal with its own Nets PSAM. The terminal is directly connected to the transmission line.
'01'	The transaction is generated in a terminal with its own Nets PSAM. The terminal is connected to a communication server via a public or private network. The communication server enables multiple terminals to share one or more transmission lines to Nets Denmark A/S.
'02'	The transaction is generated in a terminal without a Nets PSAM. The terminal is connected to a terminal server (via a public or private network) hosting one or more Nets PSAMs. The terminal server enables multiple terminals to share one or more transmission lines to Nets Denmark A/S.
'03'..'FF'	RFU

2-13.7.13 Coding of Tag 'CC' (MAD-Handler ID)

This data object (Tag 'CC') may be inserted in the header either by the PSAM or by the CAD.

2-13.7.14 Coding of Tag 'CD' (Terminal Identification)

- 2-13.7.14.1 A This data object (Tag 'CD') shall never be inserted by the CAD.

2-13.7.15 Coding of Tag 'CE' (Proprietary Data)

This data object ('CE') is reserved for proprietary data. The host will echo this data object if present in the message.

2-13.7.16 Coding of Tag 'CF' (Communication Interface Statistics)

This data object ('CF') is reserved for communication interface statistics.

- 2-13.7.16.1 A The format of the Statistic Vector shall be according to table 2-13.13 page 2-13-18.

The error counters and statistics are also defined in table 2-13.13 page 2-13-18.

- 2-13.7.16.2 A When a message from Nets Denmark arrives with a statistic vector, the communication interface shall subtracts the received counter values from the values in the appropriate counters (field 7 - 18).

NOTE: Normally this means that all the counters are reset to zero, but if an error occur before the message arrives, the counters shall still be incremented as normally.

Some counters may then contain values different from zero after the subtraction.

- 2-13.7.16.3 A If the Connection Request counter reach the maximum value (65535), the incrementing of this counter shall stop.

- | | | |
|-------------|---|----------------------------------------------------------------------------------------------------------------------|
| 2-13.7.16.4 | A | If the Connection Time counter reach the maximum value (4.294.967.295), the incrementing of this counter shall stop. |
| 2-13.7.16.5 | A | If a Connection Error counter reach the maximum value (255), the incrementing of this counter shall stop. |

2-13.7.17 Coding of Tag 'D1' (Reference STAN)

This data object ('D1') is reserved for the Reference STAN.

Reference STAN is the value of the data element STAN indicated in the response to the *Initiate Payment* command.

The notation Reference STAN is only relevant for the Transaction Requests:

- Purchase
- Refund and
- Capture

The value of tag 'D1' may be used to link any advice with financial impact to a specific Transaction Request.

Tag 'D1' will be present only if the advice has financial impact, i.e.

- the MTI is 0226 (Financial Advice) or
- the MTI is 0426 (Reversal Advice) and the original MTI was either 0206 or 0226.

The tag 'D1' is intended for report purposes, see section 1-9.25.6 page 1-9-25 Total Reports for further details.

2-13.7.18 Coding of Tag 'D2' (MTI of the Original Message)

This data object ('D2') is used to identify the MTI of the Original Message.

Tag 'D2' will only appear together with tag 'D1' (see conditions defined for tag 'D1').

Table 2-13.13 - Communication Interface - Statistic Vector

Field	Field Name	Attrib.	Value	Comments	Connection Type ¹⁾	
					1	2
1	Tag	an1	'CF'		M	M
2	Length	b1	'15'	Length of the statistic vector exclusive Tag and Length	M	M
3	Version	b1	'01'	Version of the statistic vector	M	M
4	Connection Type	b1		Directly = '01', means that the interface is directly connected to Nets Denmark Indirectly = '02', means that the interface is connected through a router	M	M
5	Certification ID	b2		Certification identification given to the communication interface by Nets Denmark.	M	M
6	Bearer Network (primary terminal interface)	b1		Unspecified = '00' ISDN = '01' GSM = '02' PSTN = '03' VPN/LAN = '04' GPRS = '05'	M	O
7	Connection Request	b2		Number of connection requests	M	M
8	Connection Time	b4		Total amount of time in seconds the interface has been connected	M	M
9	Total Connection Errors	b1		Total number of connection errors ²⁾	M	M
10	Connection Error 1	b1		Total number of "No dial tone"	M	O
11	Connection Error 2	b1		Total number of "Busy"	M	O
12	Connection Error 3	b1		Total number of "No answer"	M	O
13	Connection Error 4	b1		Total number of "No carrier"	M	O
14	Connection Error 5	b1		Total number of "Unexpected carrier lost"	M	O
15	Connection Error 6	b1		Total number of "PPP negotiation ended unsuccessfully"	M	O
16	Connection Error 7	b1		Total number of "TCP negotiation ended unsuccessfully"	M	M
17	Connection Error 8	b1		Total number of "Unexpected disconnections of the TCP connection"	M	M
18	Connection Error 9	b1		Total number of "Unexpected disconnections in the 'non-activity time-out' period" ³⁾	M	M

Legend: M = Mandatory, O = Optional, if not provided set to '00'.

¹⁾ See definition in field 4.

²⁾ Incremented when one of the specific Connection Error counters are incremented or if an error can not be categorized in one of the Connection Errors 1 – 9.

³⁾ The host is closing the connection after 30 seconds without any valid transactions (non-activity time-out).

2-13.8 Detailed Message Formats

The following tables define the contents of each APACS message type used in the OTRS environment.

NOTE: The grey areas in the following tables designate encrypted fields.

NOTE: Message formats for ICC transactions covers contact ICC as well as contactless ICC transactions. Message formats for MSC transactions covers physical magstripe as well as contactless MSD transactions.

2-13.8.1 Authorization Request Messages (0106/0116)

Table 2-13.14 - Authorization Request - ICC (Original/Extended and Supplementary)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0106"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	Present if field 35 is absent
3	Processing code		n6		3	See section 2–13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Present if field 35 is absent (From Tag '5F24')
15	GMT offset		n3		2	See section 2–13.9.3
21	POS capability code		an6		6	See section 2–13.9.4
22	POS entry mode		n6		3	See section 2–13.9.5
23	Card sequence number		n3		2	If present on ICC
24	Function code		n3		2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
30	Amount, original transaction		n12		6	If Supplementary Authorization.
35	Track 2 data	LVAR	z..37		var.	Tag '57' from ICC
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID PIN Pad id (if PIN based) Terminal Approval Number Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	Present if Online PIN. See section 2–13.9.12

Table 2-13.14 - Authorization Request - ICC (Original/Extended and Supplementary)
(concluded)

Field	Field name	Format	Attrib.	Value	Len	Comment
49	Currency code, transaction		n3		2	
52	PIN data		b8		8	Present if Online PIN. Enciphered PIN block
55	ICC system related data	LLVAR	b ..MAX		var.	See section 2-13.9.13
56	Original data elements	LVAR	b..32		26	If Supplementary Authorization. Echo from 0106-message: See section 2-13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.15 - Authorization Request Response - ICC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0116"	4	
–	Primary Message Bit Map		b8		8	
4	Amount transaction		n12		6	(Partial) Amount authorized, If supported by Issuer
11	Systems trace audit number		n6		3	Echo from 0106–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0106–message
13	Date, local transaction		n4	MMDD	2	Echo from 0106–message
15	GMT offset		n3		2	Echo from 0106–message
38	Approval code		anp6		6	If transaction is approved
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0106–message
44	Additional response data	LVAR	ans ..99		var.	Reconciliation info. At least: Card Name Auth. Response Code
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
54	Amounts, additional	LVAR	ans ..120		var.	Present if data received from Issuer. See section 2–13.9.14 Available Funds
55	ICC system related data	LLVAR	b ..MAX		var.	Present if data received from Issuer. See section 2–13.9.13
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0106–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section 2–13.9.19
64	Message authentication code		b8		8	

Table 2-13.16 - Authorization Request - MSC (Original/Extended and Supplementary)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0106"	4	
-	Primary Message Bit Map		b8		8	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
30	Amount, original transaction		n12		6	If Supplementary Authorization.
35	Track 2 data	LVAR	z..37		var.	Not if Track 3 is present
36	Track 3 data	LVAR	z104		52	Only if Track 3 is present
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID PIN Pad id (if PIN based) Terminal Approval Number Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	Present if Online PIN. See section 2-13.9.12
49	Currency code, transaction		n3		2	
52	PIN data		b8		8	Present if Online PIN. Enciphered PIN block
56	Original data elements	LVAR	b..32		26	If Supplementary Authorization. Echo from 0106-message: See section 2-13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAMCREATOR} □ ID _{PSAM}
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.17 - Authorization Request Response - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0116"	4	
-	Primary Message Bit Map		b8		8	
4	Amount transaction		n12		6	(Partial) Amount authorized, If supported by Issuer
11	Systems trace audit number		n6		3	Echo from 0106–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0106–message
13	Date, local transaction		n4	MMDD	2	Echo from 0106–message
15	GMT offset		n3		2	Echo from 0106–message
38	Approval code		anp6		6	If transaction is approved
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0106–message
44	Additional response data	LVAR	ans ..99		var.	Reconciliation info. At least: Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
54	Amounts, additional	LVAR	ans ..120		var.	Present if data received from Issuer. See section 2–13.9.14 Available Funds
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0106–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section 2–13.9.19
64	Message authentication code		b8		8	

Table 2-13.18 - Authorization Request - Key Entered (Original/Supplementary)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0106"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
30	Amount, original transaction		n12		6	If Supplementary Authorization.
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b..32		26	If Supplementary Authorization. Echo from 0106-message: See section 2-13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} <input type="checkbox"/> ID _{PSAMCREATOR} <input type="checkbox"/> ID _{PSAM}
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.19 - Authorization Request Response - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0116"	4	
–	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0106–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0106–message
13	Date, local transaction		n4	MMDD	2	Echo from 0106–message
15	GMT offset		n3		2	Echo from 0106–message
38	Approval code		anp6		6	If transaction is approved
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0106–message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0106–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section 2–13.9.19
64	Message authentication code		b8		8	

2-13.8.2 Authorization Advice Messages (0126/0136)

Table 2-13.20 - Authorization Advice - ICC (Offline Declined and Failed)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0126"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	Present if field 35 is absent
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Present if field 35 is absent
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
23	Card sequence number		n3		2	If present on ICC
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
35	Track 2 data	LVAR	z..37		var.	Tag '57' from ICC
39	Action code		n4		2	
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
49	Currency code, transaction		n3		2	'0000', if no currency is specified
55	ICC system related data	LLVAR	b..MAX		var.	See section 2-13.9.13
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAMCREATOR} □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

NOTE: Field 2 and field 14 are only present if field 35 is absent and PAN and expiration date are actual read from the ICC.

Table 2-13.21 - Authorization Advice Response - ICC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0136"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0126–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0126–message
13	Date, local transaction		n4	MMDD	2	Echo from 0126–message
15	GMT offset		n3		2	Echo from 0126–message
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0126–message
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0126–message
61	Random number	LVAR	ansb ..255		9	Echo from 0126–message Only if advice can be deleted from Data Store

Table 2-13.22 - Authorization Advice - MSC (Offline Authorization, Offline Declined and Failed)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0126"	4	
-	Primary Message Bit Map		b8		8	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
35	Track 2 data	LVAR	z ..37		var.	Not if Track 3 is present
36	Track 3 data	LVAR	z104		52	Only if Track 3 is present
39	Action code		n4		2	
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
49	Currency code, transaction		n3		2	'0000', if no currency is specified
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.23 - Authorization Advice Response - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0136"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0126–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0126–message
13	Date, local transaction		n4	MMDD	2	Echo from 0126–message
15	GMT offset		n3		2	Echo from 0126–message
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0126–message
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD_Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0126–message
61	Random number	LVAR	ansb ..255		9	Echo from 0126–message Only if advice can be deleted from Data Store

Table 2-13.24 - Authorization Advice - Key Entered (Offline Declined and Failed)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0126"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
39	Action code		n4		2	
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	'0000', if no currency is specified
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAMCREATOR} □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

NOTE: Field 2 and field 14 are only present if field 35 is absent and PAN and expiration date are given in the response to the *Get Merchant Data* command.

Table 2-13.25 - Authorization Advice Response - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0136"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0126–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0126–message
13	Date, local transaction		n4	MMDD	2	Echo from 0126–message
15	GMT offset		n3		2	Echo from 0126–message
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0126–message
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0126–message
61	Random number	LVAR	ansb ..255		9	Echo from 0126–message Only if advice can be deleted from Data Store

2-13.8.3 Financial Request Messages (0206/0216)

Table 2-13.26 - Financial Request - ICC (Refund)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0206"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	Not present if field35 is present
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Not present if field35 is present
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3	200	2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
35	Track 2 data	LVAR	z..37		var.	Tag '57' if present in ICC
37	Retrieval reference number		anp12		12	Batch number
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
49	Currency code, transaction		n3		2	
59	Additional Data Capture	LLVAR	ansb..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
62	Merchant Initiative	LVAR	ansb..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

NOTE: An ICC (Refund) transaction can either be initiated as a Financial Request or a Financial Advice (in case of offline)

Table 2-13.27 - Financial Request Response - ICC (Refund)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0216"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0206–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0206–message
13	Date, local transaction		n4	MMDD	2	Echo from 0206–message
15	GMT offset		n3		2	Echo from 0206–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
38	Approval code		anp6		6	If transaction is approved
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0206–message
44	Additional response data	LVAR	ans ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name, see 2–13.9.10
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0206–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section 2–13.9.19
64	Message authentication code		b8		8	

Table 2-13.28 - Financial Request - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0206"	4	
-	Primary Message Bit Map		b8		8	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3	200	2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
35	Track 2 data	LVAR	z ..37		var.	Not if Track 3 is present
36	Track 3 data	LVAR	z104		52	Only if Track 3 is present
37	Retrieval reference number		anp12		12	Batch number
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID PIN Pad id (if PIN based) Terminal Approval Number Grand Total PSAM Version
47	Additional data - national	LVAR	ans ..255		var.	Present if Online PIN. See section 2-13.9.12
49	Currency code, transaction		n3		2	
52	PIN data		b8		8	Present if Online PIN. Enciphered PIN block
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.29 - Financial Request Response - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0216"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0206–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0206–message
13	Date, local transaction		n4	MMDD	2	Echo from 0206–message
15	GMT offset		n3		2	Echo from 0206–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
38	Approval code		anp6		6	If transaction is approved
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0206–message
44	Additional response data	LVAR	ans ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name,
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0206–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section 2–13.9.19
64	Message authentication code		b8		8	

Table 2-13.30 - Financial Request - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0206"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3	200	2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
37	Retrieval reference number		anp12		12	Batch number
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
47	Additional data - national	LVAR	ansb ..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAMCREATOR} □ ID _{PSAM}
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.31 - Financial Request Response - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0216"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0206–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0206–message
13	Date, local transaction		n4	MMDD	2	Echo from 0206–message
15	GMT offset		n3		2	Echo from 0206–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
38	Approval code		anp6		6	If transaction is approved
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0206–message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0206–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section 2–13.9.19
64	Message authentication code		b8		8	

2-13.8.4 Financial Advice Messages (0226/0236)

Table 2-13.32 - Financial Advice - ICC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0226"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	Present if field 35 is absent
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Present if field 35 is absent
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
23	Card sequence number		n3		2	If present on ICC
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
30	Amount, original transaction		n12		6	Only present if field 24 is 202 (Amount differs)
35	Track 2 data	LVAR	z..37		var.	Tag '57' if present in ICC
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if online authorized against Acquirer host
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
47	Additional data – national	LVAR	ansb..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	
55	ICC system related data	LLVAR	b..MAX		var.	See section 2-13.9.13
56	Original data elements	LVAR	b..32		26	Present if online authorized: Echo from 0106-message: See section 2-13.9.14
59	Additional Data Capture	LLVAR	ansb..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb..255		14	RID _{PSAM} □ID _{PSAM} CREATOR □ID _{PSAM}

Table 2-13.33 - Financial Advice - ICC (*concluded*)

Field	Field name	Format	Attrib.	Value	Len	Comment
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.34 - Financial Advice Response - ICC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0236"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0226–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0226–message
13	Date, local transaction		n4	MMDD	2	Echo from 0226–message
15	GMT offset		n3		2	Echo from 0226–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0226–message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message Only if advice can be deleted from Data Store

Table 2-13.35 - Financial Advice - ICC (Refund, offline)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0226"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	Present if field 35 is absent
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Present if field 35 is absent
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3	200	2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
35	Track 2 data	LVAR	z..37		var.	Tag '57' if present in ICC
37	Retrieval reference number		anp12		12	Batch number
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
47	Additional data - national	LVAR	ansb ..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

NOTE: An ICC (Refund) transaction can either be initiated as a Financial Request or a Financial Advice (in case of offline)

Table 2-13.36 - Financial Advice Response - ICC (Refund, offline)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0236"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0226–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0226–message
13	Date, local transaction		n4	MMDD	2	Echo from 0226–message
15	GMT offset		n3		2	Echo from 0226–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0226–message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message Only if advice can be deleted from Data Store

Table 2-13.37 - Financial Advice - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0226"	4	
-	Primary Message Bit Map		b8		8	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
30	Amount, original transaction		n12		6	Only present if field 24 is 202 (Amount differs)
35	Track 2 data	LVAR	z ..37		var.	Not if Track 3 is present
36	Track 3 data	LVAR	z104		52	Only if Track 3 is present
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if online authorized against Acquirer host
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b ..32		26	Present if authorized: Echo from 0106-message: See section 2-13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.38 - Financial Advice Response - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0236"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0226–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0226–message
13	Date, local transaction		n4	MMDD	2	Echo from 0226–message
15	GMT offset		n3		2	Echo from 0226–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0226–message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message Only if advice can be deleted from Data Store

Table 2-13.39 - Financial Advice - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0226"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	
3	Processing code		n6		3	See section 2-13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	
15	GMT offset		n3		2	See section 2-13.9.3
21	POS capability code		an6		6	See section 2-13.9.4
22	POS entry mode		n6		3	See section 2-13.9.5
24	Function code		n3		2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
30	Amount, original transaction		n12		6	Only present if field 24 is 202 (Amount differs)
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if online authorized against Acquirer host
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2-13.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b..32		26	Present if online authorized: Echo from 0106-message: See section 2-13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.40 - Financial Advice Response - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0236"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0226–message
12	Time, local transaction		n6	hhmmss	3	Echo from 0226–message
13	Date, local transaction		n4	MMDD	2	Echo from 0226–message
15	GMT offset		n3		2	Echo from 0226–message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0226–message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message Only if advice can be deleted from Data Store

2-13.8.5 PSAM Update and Reconciliation Report Messages (0360/364/0370/374)

Table 2-13.41 - File Action Instruction, PSAM Update

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0360"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	300	2	See section 2–13.9.6
27	Download control		n6		3	See section 2–13.9.8
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAMCREATOR} □ ID _{PSAM}
63	PSAM update	LLVAR	ansb ..MAX		var.	See section 2–13.9.19

Table 2-13.42 - File Action Instruction, Reconciliation Report

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0364"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	380	2	See section 2-13.9.6
27	Download control		n6		3	See section 2-13.9.8
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} <input type="checkbox"/> ID _{PSAM} CREATOR <input type="checkbox"/> ID _{PSAM}
63	File Data (Recon report)	LLVAR	ansb ..MAX		var.	See section 2-13.9.19

Table 2-13.43 - File Action Instruction Acknowledgement, PSAM Update

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0370"	4	
-	Primary Message Bit Map		b8		8	
27	Download control		n6		3	See section 2-13.9.8
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} <input type="checkbox"/> ID _{PSAM} CREATOR <input type="checkbox"/> ID _{PSAM}

Table 2-13.44 - File Action Instruction Acknowledgement, Reconciliation Report

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0374"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	380	2	See section 2-13.9.6
27	Download control		n6		3	See section 2-13.9.8
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} <input type="checkbox"/> ID _{PSAM} CREATOR <input type="checkbox"/> ID _{PSAM}

2-13.8.6 Reversal Advice Messages (0426/0436)

Table 2-13.45 - Reversal Advice - ICC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0426"	4	
–	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n ..19		var.	Present if field 35 is absent
3	Processing code		n6		3	See section 2–13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Present if field 35 is absent
15	GMT offset		n3		2	See section 2–13.9.3
21	POS capability code		an6		6	See section 2–13.9.4
22	POS entry mode		n6		3	See section 2–13.9.5
23	Card sequence number		n3		2	If present on ICC
24	Function code		n3		2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
35	Track 2 data	LVAR	z ..37		var.	Tag '57' if present in ICC
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if Authorization Response was received
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2–13.9.12
49	Currency code, transaction		n3		2	
55	ICC system related data	LLVAR	b ..MAX		var.	See section 2–13.9.13
56	Original data elements	LVAR	b ..32		26	Echo from 0106/0226–msg.: See section 2–13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAMCREATOR} □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	

Table 2-13.46 - Reversal Advice - ICC (*concluded*)

Field	Field name	Format	Attrib.	Value	Len	Comment
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.47 - Reversal Advice Response - ICC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0436"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0426-message
12	Time, local transaction		n6	hhmmss	3	Echo from 0426-message
13	Date, local transaction		n4	MMDD	2	Echo from 0426-message
15	GMT offset		n3		2	Echo from 0426-message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Echo from 0426-message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426-message
61	Random number	LVAR	ansb ..255		9	Echo from 0426-message Only if advice can be deleted from Data Store

Table 2-13.48 - Reversal Advice - ICC (Refund)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0426"	4	
–	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n ..19		var.	Present if field 35 is absent
3	Processing code		n6		3	See section 2–13.9.2
4	Amount, transaction		n12		6	
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	Present if field 35 is absent
15	GMT offset		n3		2	See section 2–13.9.3
21	POS capability code		an6		6	See section 2–13.9.4
22	POS entry mode		n6		3	See section 2–13.9.5
24	Function code		n3		2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
35	Track 2 data	LVAR	z ..37		var.	Tag '57' if present in ICC
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if Authorization Response was received
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2–13.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b ..32		26	Echo from 0106/0226–msg.: See section 2–13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} <input type="checkbox"/> ID _{PSAM} CREATOR <input type="checkbox"/> ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.49 - Reversal Advice Response - ICC (Refund)

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0436"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0426-message
12	Time, local transaction		n6	hhmmss	3	Echo from 0426-message
13	Date, local transaction		n4	MMDD	2	Echo from 0426-message
15	GMT offset		n3		2	Echo from 0426-message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Echo from 0426-message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426-message
61	Random number	LVAR	ansb ..255		9	Echo from 0426-message Only if advice can be deleted from Data Store

Table 2-13.50 - Reversal Advice - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0426"	4	
–	Primary Message Bit Map		b8		8	
3	Processing code		n6		3	See section 2–13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
15	GMT offset		n3		2	See section 2–13.9.3
21	POS capability code		an6		6	See section 2–13.9.4
22	POS entry mode		n6		3	See section 2–13.9.5
24	Function code		n3		2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
35	Track 2 data	LVAR	z ..37		var.	Not if Track 3 is present
36	Track 3 data	LVAR	z104		52	Only if Track 3 is present
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if Authorization Response was received
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
47	Additional data – national	LVAR	ansb ..255		var.	See section 2–13.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b..32		26	Echo from 0106/0206/0226–msg.: See section 2–13.9.14
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} <input type="checkbox"/> ID _{PSAM} CREATOR <input type="checkbox"/> ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.51 - Reversal Advice Response - MSC

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0436"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0426-message
12	Time, local transaction		n6	hhmmss	3	Echo from 0426-message
13	Date, local transaction		n4	MMDD	2	Echo from 0426-message
15	GMT offset		n3		2	Echo from 0426-message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Echo from 0426-message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426-message
61	Random number	LVAR	ansb ..255		9	Echo from 0426-message Only if advice can be deleted from Data Store

Table 2-13.52 - Reversal Advice - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0426"	4	
-	Primary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n..19		var.	
3	Processing code		n6		3	See section 2–13.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	Only present if cashback
11	Systems trace audit number		n6		3	Unique per transaction
12	Time, local transaction		n6	hhmmss	3	
13	Date, local transaction		n4	MMDD	2	
14	Date, expiration		n4	YYMM	2	
15	GMT offset		n3		2	See section 2–13.9.3
21	POS capability code		an6		6	See section 2–13.9.4
22	POS entry mode		n6		3	See section 2–13.9.5
24	Function code		n3		2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	Present if Authorization Response was received
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb..255		var.	At least: MAD–Handler ID Terminal Approval Number Application Status Words Grand Total PSAM Version
47	Additional data – national	LVAR	ansb..255		var.	See section 2–13.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b..32		26	Echo from 0106/0206/0226–msg.: See section 2–13.9.14
59	Additional Data Capture	LLVAR	ansb..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb..255		14	RID _{PSAM} □ID _{PSAM} CREATOR □ID _{PSAM}
61	Random number	LVAR	ansb..255		9	
62	Merchant Initiative	LVAR	ansb..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table 2-13.53 - Reversal Advice Response - Key Entered

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0436"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0426-message
12	Time, local transaction		n6	hhmmss	3	Echo from 0426-message
13	Date, local transaction		n4	MMDD	2	Echo from 0426-message
15	GMT offset		n3		2	Echo from 0426-message
28	Date, reconciliation		n6	YYMMDD	3	
29	Reconciliation indicator		n3		2	Subdivision of field 28.
39	Action code		n4		2	See section 2-13.9.9
41	Card accepting device id.		an8		8	Echo from 0426-message
44	Additional response data	LVAR	ansb ..99		var.	Reconciliation info. At least: Card recon. counter id Card recon. counter name Card Name
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
59	Additional Data Capture	LLVAR	ansb ..MAX		var.	Present if Extended Issuer Envelope Data is present
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426-message
61	Random number	LVAR	ansb ..255		9	Echo from 0426-message Only if advice can be deleted from Data Store

2-13.8.7 Addendum Record Messages (0624/0634)

Table 2-13.54 - Administrative Advice - Addendum Record

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0624"	4	
–	Primary Message Bit Map		b8		8	
1	Secondary Message Bit Map		b8		8	
2	Primary account number (PAN)	LVAR	n ..19		var.	Same as in financial request/ advice
11	Systems trace audit number		n6		3	Unique per transaction
24	Function code		n3	680	2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
37	Retrieval reference number		anp12		12	Batch number
41	Card accepting device id.		an8		8	Terminal Identification
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number PSAM Version
56	Original data elements	LVAR	b..32		26	Echo from 0106/0206–msg.: See section 2–13.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ID _{PSAM} CREATOR □ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
71	Message number		n8		4	See section 2–13.9.20
72	Data record	LLVAR	ansb ..MAX		var.	See section 2–13.9.21
128	Message authentication code		b8		8	

Table 2-13.55 - Administrative Advice Response - Addendum Record

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0634"	4	
–	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0624–message
39	Action code		n4		2	See section 2–13.9.9
41	Card accepting device id.		an8		8	Echo from 0624–message
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0624–message
61	Random number	LVAR	ansb ..255		9	Echo from 0624–message Only if advice can be deleted from Data Store

2-13.8.8 Service Record Messages (0624/0634)

Table 2-13.56 - Administrative Advice - Service Record

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0624"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Unique per transaction
24	Function code		n3	690/691	2	See section 2-13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number PSAM Version Update Result(s)
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} □ ID _{PSAM} CREATOR □ ID _{PSAM}
61	Random number	LVAR	ansb ..255		9	
64	Message authentication code		b8		8	

Table 2-13.57 - Administrative Advice Response - Service Record

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0634"	4	
-	Primary Message Bit Map		b8		8	
11	Systems trace audit number		n6		3	Echo from 0624-message
39	Action code		n4		2	See section 2-13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0624-message
61	Random number	LVAR	ansb ..255		9	Echo from 0624-message Only if advice can be de- leted from Data Store

2-13.8.9 Clock Synchronization Messages (0804/0814)

Table 2-13.58 - Network Management Request - Clock Synchronization

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	852	2	See section 2–13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number

Table 2-13.59 - Network Management Request Response - Clock Synchronization

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2–13.9.3
39	Action code		n4		2	See section 2–13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number

2-13.8.10 Installation Messages (0804/0814)

Table 2-13.60 - Network Management Request - Installation, old format

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
21	POS capability code		an6		6	See section 2-13.9.4
24	Function code		n3	880	2	See section 2-13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Capabilities Additional Terminal Capabilities Software Version Number Hardware Version Number Terminal Approval Number Terminal Type Info Level PSAM Version
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAMCREATOR} ID _{PSAM}
64	Message authentication code		b8		8	

Table 2-13.61 - Network Management Request - Installation, new format ¹⁾

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
21	POS capability code		an6		6	See section 2-13.9.4
24	Function code		n3	880	2	See section 2-13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Capabilities Additional Terminal Capabilities Software Version Number Hardware Version Number Terminal Approval Number Terminal Type Info Level PSAM Version Optional: PTS Request Data PCI Data PSAM Parameters
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAMCREATOR} ID _{PSAM}
64	Message authentication code		b8		8	

NOTE: 1) The new format installation is applicable to PSAM 08.00.06 and forward when using the PTS scheme.

Table 2-13.62 - Network Management Request Response - Installation, old format

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2–13.9.3
39	Action code		n4		2	See section 2–13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0804–message
64	Message authentication code		b8		8	

Table 2-13.63 - Network Management Request Response - Installation, new format ¹⁾

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2–13.9.3
39	Action code		n4		2	See section 2–13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number Optional: PTS Response Data
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0804–message
64	Message authentication code		b8		8	

NOTE: 1) The new format installation is applicable to PSAM 08.00.06 and forward when using the PTS scheme.

2-13.8.11 Advice Transfer Messages (0804/0814)

Table 2-13.64 - Network Management Request - Advice Transfer

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	882	2	See section 2-13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number

Table 2-13.65 - Network Management Request Response - Advice Transfer

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2-13.9.3
39	Action code		n4		2	See section 2-13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number

2-13.8.12 PSAM Update Messages (0804/0814/0844)

Table 2-13.66 - Network Management Request - PSAM Update

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	884	2	See section 2–13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAMCREATOR} ID _{PSAM}

Table 2-13.67 - Network Management Request Response - PSAM Update

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2–13.9.3
39	Action code		n4		2	See section 2–13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0804/0805–mes- sage

Table 2-13.68 - Network Management Notification - PSAM Update

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0844"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	851	2	See section 2–13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAMCREATOR} ID _{PSAM}

2-13.8.13 PSAM Deactivation Messages (0804/0814)

Table 2-13.69 - Network Management Request - PSAM Deactivation

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	886	2	See section 2-13.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number PSAM Version
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAMCREATOR} ID _{PSAM}
64	Message authentication code		b8		8	

Table 2-13.70 - Network Management Request Response - PSAM Deactivation

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2-13.9.3
39	Action code		n4		2	See section 2-13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0804-message
63	PSAM update	LLVAR	ansb ..MAX		var.	May be present See section 2-13.9.19

2-13.8.14 Reconciliation Messages (0804/0814/844)

Table 2-13.71 - Network Management Request - Generate Reconciliation

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	888	2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAM} CREATOR ID _{PSAM}

Table 2-13.72 - Network Management Request Response - Generate Reconciliation

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2–13.9.3
25	Message reason code		n4		2	Echo from 0804/0805–mes- sage
29	Reconciliation indicator		n3		2	Number on report generated
39	Action code		n4		2	See section 2–13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0804/0805–mes- sage

Table 2-13.73 - Network Management Request - Reconciliation Report

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0804"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	889	2	See section 2–13.9.6
25	Message reason code		n4		2	See section 2–13.9.7
29	Reconciliation indicator		n3		2	Number on report requested
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAM} CREATOR ID _{PSAM}

Table 2-13.74 - Network Management Request Response - Reconciliation Report

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0814"	4	
-	Primary Message Bit Map		b8		8	
12	Time, local transaction		n6	hhmmss	3	Host timestamp
13	Date, local transaction		n4	MMDD	2	Host timestamp
15	GMT offset		n3		2	See section 2-13.9.3
29	Reconciliation indicator		n3		2	Number on report generated
39	Action code		n4		2	See section 2-13.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0804/0805-mes- sage

Table 2-13.75 - Network Management Notification - Reconciliation Report

Field	Field name	Format	Attrib.	Value	Len	Comment
MTI	Message Type Identifier		an4	"0844"	4	
-	Primary Message Bit Map		b8		8	
24	Function code		n3	890	2	See section 2-13.9.6
25	Message reason code		n4		2	See section 2-13.9.7
29	Reconciliation indicator		n3		2	Number on report generated
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD-Handler ID Terminal Approval Number
60	PSAM identifier	LVAR	ansb ..255		14	RID _{PSAM} ID _{PSAM} CREATOR ID _{PSAM}

NOTE: The following Action codes Codes may be returned from the Host.

- 0008 Reconciliation restarted
- 5406 Reconciliation already activated
- 5412 Reconciliation did not succeed, try later.
- 6013 The report has been generated, fetch report.
- 6022 The report requested does not exist.

2-13.9 Coding of Application Specific Fields

2-13.9.1 Coding Conventions

TLV Coding for APACS fields

This coding applies to the following fields:

- 44: Additional Response Data
- 46: CAD Management/Service Quality Data
- 47: Additional Data - National
- 59: Additional Data - Capture
- 63: PSAM Updates
- 72: Addendum Record/Reconciliation information

Subfields identified by tags do not have a fixed position in the record. In some cases there may even be more than one instance with the same tag.

Each subfield consists of the following three elements:

- Tag (an2)
- Length (b2)
- Value (type and length defined by tag and length fields)

As an example,

Tag	Item	Attrib.	Value
II	Person-name	an11	"Hans Hansen"
IM	No-of-passengers	n3	5

will be coded as:

```
"I1" '000B' "Hans HansenIM" '00020005'.
```

NOTE: This coding is different from the TLV coding used in Field 55 (ICC system related data).

2-13.9.2 Coding of Field 3 (Processing Code)

This 6-digit field consists of three subfields. Position 1-2 describe a specific transaction type, position 3-4 describe the debit account type affected by the transaction and position 5-6 describe the credit account affected.

For this system, only position 1-4 are used (position 5-6 are set to zero).

Table 2-13.76 - Applicable values for position 1-2 of Field 3 (Processing Code)

Value	Description
00xxxx–19xxxx	Debits
00xx00	Goods and services
01xx00	Cash
02xx00	Adjustment
09xx00	Goods and services with cashback
11xx00	Quasi-cash and script
20xxxx–29xxxx	Credits
20xx00	Returns/Refunds
22xx00	Adjustment

Table 2-13.77 - Applicable values for position 3-4 of Field 3 (Processing Code)

Value	Description
xx0000–xx6000	Account Type
xx0000	Default account – unspecified
xx1000	Savings account
xx2000	Check/debit account
xx3000	Credit account

2-13.9.3 Coding of Field 15 (GMT Offset)

This 3-digit field consists of two subfields. Digit 1 defines the direction and increment of the offset from GMT. Digits 2-3 define the magnitude of the offset (number of increments).

Table 2-13.78 - Applicable values for Field 15 (GMT Offset), position 1

Value	Description
0	Positive (ahead of GMT). Offset in 1 hour increments
1	Negative (behind GMT). Offset in 1 hour increments
2	Positive (ahead of GMT). Offset in 15 minute increments
3	Negative (behind GMT). Offset in 15 minute increments
4	Positive (ahead of GMT). Offset in 15 minute increments. Participates in daylight savings time
5	Negative (behind GMT). Offset in 15 minute increments. Participates in daylight savings time

Depending on the value of position 1, the valid values for position 2-3 are either 0-12 or 0-48.

The values used in this system are further described in section 2-5.13.5 page 2-5-97, Clock Synchronization.

2-13.9.4 Coding of Field 21 (POS Capability Code)

This 6-character field consists of six individually coded subfields. The following tables define the applicable values for this system. Valid combinations can be found in table 2-13.94 page 2-13-73.

Position 1 defines the *primary* card data input capability.

Table 2-13.79 - Applicable values for Field 21 (POS Capability Code), position 1

Value	Description
0	Unknown
1	Not available
2	Magnetic stripe read
5	ICC
6	Key Entered
P	Contactless Only

Position 2 defines the *primary* cardholder authentication capability.

Table 2-13.80 - Applicable values for Field 21 (POS Capability Code), position 2

Value	Description
0	No electronic authentication
1	PIN

Position 3 defines the CAD security capability.

Table 2-13.81 - Applicable values for Field 21 (POS Capability Code), position 3

Value	Description
2	No card capture capability. MAC capability (by the PSAM)
3	Card capture capability. MAC capability (by the PSAM)

Position 4 defines the card data output capability.

Table 2-13.82 - Applicable values for Field 21 (POS Capability Code), position 4

Value	Description
0	Unknown
1	None
2	Magnetic stripe write
3	ICC

Position 5 defines the CAD output capability.

Table 2-13.83 - Applicable values for Field 21 (POS Capability Code), position 5

Value	Description
0	Unknown
1	None
2	Print, general
3	Display, general
4	Print and display, general
5	Print, cardholder only
6	Display, cardholder only
7	Print and display, cardholder only
8	Print, card acceptor only
9	Display, card acceptor only
A	Print and display, card acceptor only
B	Print, card acceptor and cardholder
C	Display, card acceptor and cardholder
D	Print and display, card acceptor and cardholder

Position 6 defines the PIN capture capability.

Table 2-13.84 - Applicable values for Field 21 (POS Capability Code), position 6

Value	Description
0	No PIN capture capability
1	Device PIN capture capability unknown
C	Twelve characters (digits)

Valid values for Field 21 (POS Capability Code)

Depending of the actual implementation of the terminal, two different sets of POS Capability Codes are defined. These sets are named "Flex Terminal Capability Mark III - IV". Terminals without ICC reader, "Flex Terminal Capability Mark I - II", are no longer permitted.

Table 2-13.85 - Flex Terminal Capability Mark IV

Flex Terminal Capability Mark IV		Full grade OTRS implementation (supporting PIN Pad and ICC reader)
Position	Value	Description
1	5	Primary card data input: ICC
2	1	Primary cardholder authentication: PIN
3	2 or 3	Card capture: 2 = No, 3 = Yes
4	3	Card data output: ICC
5	4	Print and Display: General
6	C	PIN capture: 12 digits

Table 2-13.86 - Flex Terminal Capability Mark III

Flex Terminal Capability Mark III		Terminal without PIN Pad, but with ICC reader
Position	Value	Description
1	5	Primary card data input: ICC
2	0	Primary cardholder authentication: No electronic authentication
3	2 or 3	Card capture: 2 = No, 3 = Yes
4	3	Card data output: ICC
5	4	Print and Display: General
6	0	PIN capture: No PIN capture capability

2-13.9.5 Coding of Field 22 (POS Entry Mode)

This 6-character field consists of six individually coded sub-fields. The following tables define the applicable values for this system. Valid combinations to be conveyed in the *Initiate Payment* command can be found in table 2-13.93 page 2-13-72 and 2-13.94 page 2-13-73.

Position 1 defines the operating environment.

Table 2-13.87 - Applicable values for Field 22 (POS Entry Mode), position 1

Value	Description
0	Not available
1	On premises of card acceptor, attended
2	On premises of card acceptor, unattended
3	Off premises of card acceptor, attended
4	Off premises of card acceptor, unattended
5	On premises of cardholder, unattended
7	On premises of card acceptor, attended – <i>not</i> authorized
8	UPT level 2 – no PIN – online only
9	UPT level 3 – no PIN – offline

Position 2 defines the cardholder presence.

Table 2-13.88 - Applicable values for Field 22 (POS Entry Mode), position 2

Value	Description
0	Cardholder present
1	Cardholder not present, unspecified
2	Cardholder not present, mail order
3	Cardholder not present, telephone order
4	Cardholder not present, standing authorization
5	Fallback processing

Position 3 defines the card data input mode.

Table 2-13.89 - Applicable values for Field 22 (POS Entry Mode), position 3

Value	Description
0	Unspecified
2	Magnetic stripe read
3	Proximity Payment using Chip rules
4	Proximity Payment using Magstripe rules
5	ICC
6	Key entered
7	Magnetic stripe read after ICC malfunction

Position 4 defines the cardholder authentication mode.

Table 2-13.90 - Applicable values for Field 22 (POS Entry Mode), position 4

Value	Description
0	Not authenticated
1	PIN
5	Manual signature verification
6	Other manual verification (e.g. driver's license)
7	Address verification (mail order/telephone order)
8	On Device CVM/Consumer Device CVM

Position 5 defines the cardholder authentication entity.

Table 2-13.91 - Applicable values for Field 22 (POS Entry Mode), position 5

Value	Description
0	Not authenticated
1	ICC
2	CAD
3	Authorizing agent
4	Merchant
5	Other
6	Mobile Device

Position 6 defines the CAD output status.

Table 2-13.92 - Applicable values for Field 22 (POS Entry Mode), position 6

Value	Description
0	Unknown
1	None
2	Printer(s) not operational
3	Display(s) not operational
4	Printer(s) and display(s) not operational
8	PIN Pad not operational

- 2-13.9.5.1 A Depending of the terminal environment and the Card Data Source, the terminal shall code the POS Entry Mode in the *Initiate Payment* command according to table 2-13.93.

NOTE: Additional information related to the MTI can be found in table 2-13.94.

Table 2-13.93 - POS Entry Mode Values to be Inserted in the *Initiate Payment* Command

Terminal Environment	Card Data Source						
	ICC	Contactless		MSC		Key Entered	Token
		ICC	MSD	MSC	MSC (fallback)		
Attended	10500X	10300X	10400X	10200X	10700X	10600X	10000X
Mail order						12600X	12000X
Telephone order						13600X	13000X
UPT level 1	20500X	20300X	20400X	20200X	20700X		20000X
UPT level 2	80500X	80300X	80400X	80200X	80700X		80000X
UPT level 3	90500X	90300X	90400X	90200X	90700X		90000X
<p>Legend: Coding of the POS Entry Mode. Position 1 is the leftmost position, position 6 the rightmost. X = don't care.</p> <p>For the Terminal Environment the following supported Terminal Types apply: Attended: 11, 21, 22, 23 UPT level 1: 24, 25 UPT level 2: 25 (No CVM) UPT level 3: 26</p> <p>Post Purchase and Post Refund apply to the Attended/Token value (10000X).</p>							

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode

				ISO 8583				APACS 60											
Environment	CVM	MTI	Transaction	POS Data Code				POS Capabil- ity Code, field 21:	POS Entry Mode, field 22:										
ICC																			
Attended	Online PIN	0106		51X	101	510	34C	5	1	X	3	4	C	1	0	5	1	0	X
		0126	Error	51X	101	510	11C	5	1	X	3	4	C	7	0	5	1	0	X
		0226	Authorized	51X	101	515	34C	5	1	X	3	4	C	1	0	5	1	5	X
		0426	Reversal (0106)	51X	101	515	34C	5	1	X	3	4	C	1	0	5	1	5	X
	Offline PIN	0106		51X	101	511	34C	5	1	X	3	4	C	1	0	5	1	1	X
		0126	Error	51X	101	500	11C	5	1	X	3	4	C	7	0	5	0	1	X
		0126	Offline Auth.	51X	101	511	34C	5	1	X	3	4	C	1	0	5	1	1	X
		0226	Authorized	51X	101	511	34C	5	1	X	3	4	C	1	0	5	1	1	X
		0226	Not authorized	51X	101	511	11C	5	1	X	3	4	C	7	0	5	1	1	X
		0426	Reversal (0106)	51X	101	511	11C	5	1	X	3	4	C	7	0	5	1	1	X
	Signature	0106		51X	101	550	34C	5	1	X	3	4	C	1	0	5	5	0	X
		0106		51X	101	550	11C	5	1	X	3	4	C	7	0	5	5	0	X
		0126	Offline Auth.	51X	101	550	34C	5	1	X	3	4	C	1	0	5	5	0	X
		0206	(ICC Refund)	51X	101	550	34C	5	1	X	3	4	C	1	0	5	5	0	X
		0226	Authorized	51X	101	554	34C	5	1	X	3	4	C	1	0	5	5	4	X
		0226	Not authorized	51X	101	554	11C	5	1	X	3	4	C	7	0	5	5	4	X
		0426	Reversal (0106)	51X	101	554	34C	5	1	X	3	4	C	1	0	5	5	4	X
		0426	Reversal (0106)	51X	101	554	11C	5	1	X	3	4	C	7	0	5	5	4	X
	No CVM (Card present)	0106		51X	101	500	34C	5	1	X	3	4	C	1	0	5	0	0	X
		0126	Offline Auth.	51X	101	500	34C	5	1	X	3	4	C	1	0	5	0	0	X
		0226	Authorized	51X	101	500	34C	5	1	X	3	4	C	1	0	5	0	0	X
		0226	Not authorized	51X	101	500	11C	5	1	X	3	4	C	7	0	5	0	0	X
		0426	Reversal (0106)	51X	101	500	11C	5	1	X	3	4	C	7	0	5	0	0	X
	Combined (Offline PIN & Signature)	0106		51X	101	511	34C	5	1	X	3	4	C	1	0	5	1	1	X
		0126	Offline Auth.	51X	101	511	34C	5	1	X	3	4	C	1	0	5	1	1	X
		0226	Authorized	51X	101	511	34C	5	1	X	3	4	C	1	0	5	1	1	X
		0226	Not authorized	51X	101	511	11C	5	1	X	3	4	C	7	0	5	1	1	X
		0226	Not authorized	51X	101	511	11C	5	1	X	3	4	C	7	0	5	1	4	X
0426		Reversal (0106)	51X	101	511	11C	5	1	X	3	4	C	7	0	5	1	1	X	

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode
(continued)

				ISO 8583				APACS 60		
Environment	CVM	MTI	Transaction	POS Data Code				POS Capabil- ity Code, field 21:	POS Entry Mode, field 22:	
ICC										
CAT-1	Online PIN	0106		51X	201	510	34C	5 1 X 3 4 C	2 0 5 1 0 X	
		0226	Authorized	51X	201	515	34C	5 1 X 3 4 C	2 0 5 1 5 X	
		0426	Reversal (0106)	51X	201	515	34C	5 1 X 3 4 C	2 0 5 1 5 X	
	Offline PIN	0106		51X	201	511	34C	5 1 X 3 4 C	2 0 5 1 1 X	
		0126	Offline Auth.	51X	201	511	34C	5 1 X 3 4 C	2 0 5 1 1 X	
		0226	Authorized	51X	201	511	34C	5 1 X 3 4 C	2 0 5 1 1 X	
		0226	Not authorized	51X	201	511	34C	5 1 X 3 4 C	2 0 5 1 1 X	
	No CVM	0106		51X	201	500	34C	5 1 X 3 4 C	2 0 5 0 0 X	
		0126	Offline Auth.	51X	201	500	34C	5 1 X 3 4 C	2 0 5 0 0 X	
		0226	Authorized	51X	201	500	34C	5 1 X 3 4 C	2 0 5 0 0 X	
		0226	Not authorized	51X	201	500	34C	5 1 X 3 4 C	2 0 5 0 0 X	
	CAT-2	No CVM	0106		50X	N01	500	340	5 0 X 3 4 0	8 0 5 0 0 X
0126			Offline Auth.	50X	N01	500	340	5 0 X 3 4 0	8 0 5 0 0 X	
0226			Authorized	50X	N01	500	340	5 0 X 3 4 0	8 0 5 0 0 X	
0226			Not authorized	50X	N01	500	340	5 0 X 3 4 0	8 0 5 0 0 X	
CAT-3	No CVM	0126	Offline Auth.	50X	O01	500	110	5 0 X 3 4 0	9 0 5 0 0 X	
		0226	Not authorized	50X	O01	500	110	5 0 X 3 4 0	9 0 5 0 0 X	
MSC										
Attended	Online PIN	0106		51X	101	J10	14C	5 1 X 3 4 C	1 0 2 1 0 X	
		0126	Error	51X	101	J10	11C	5 1 X 3 4 C	7 0 2 1 0 X	
		0206		51X	101	J10	14C	5 1 X 3 4 C	1 0 2 1 0 X	
		0226	Authorized	51X	101	J15	14C	5 1 X 3 4 C	1 0 2 1 5 X	
		0426	Reversal (0106)	51X	101	J15	14C	5 1 X 3 4 C	1 0 2 1 5 X	
	Signature	0106		51X	101	J50	14C	5 1 X 3 4 C	1 0 2 5 0 X	
		0106		51X	101	J50	11C	5 1 X 3 4 C	7 0 2 5 0 X	
		0126	Offline Auth.	51X	101	J50	14C	5 1 X 3 4 C	1 0 2 5 0 X	
		0206	(ICC Refund)	51X	101	J50	14C	5 1 X 3 4 C	1 0 2 5 0 X	
		0226	Authorized	51X	101	J54	14C	5 1 X 3 4 C	1 0 2 5 4 X	
		0226	Not authorized	51X	101	J54	11C	5 1 X 3 4 C	7 0 2 5 4 X	
		0426	Reversal (0106)	51X	101	J54	14C	5 1 X 3 4 C	1 0 2 5 4 X	
		0426	Reversal (0106)	51X	101	J54	11C	5 1 X 3 4 C	7 0 2 5 4 X	

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode
(continued)

				ISO 8583				APACS 60		
Environment	CVM	MTI	Transaction	POS Data Code				POS Capabil- ity Code, field 21:	POS Entry Mode, field 22:	
MSC										
Attended	No CVM	0106		51X	101	J00	14C	5 1 X 3 4 C	1 0 2 0 0 X	
		0126	Offline Auth.	51X	101	J00	14C	5 1 X 3 4 C	1 0 2 0 0 X	
		0206		51X	101	J00	14C	5 1 X 3 4 C	1 0 2 0 0 X	
		0226	Authorized	51X	101	J00	14C	5 1 X 3 4 C	1 0 2 0 0 X	
		0226	Not authorized	51X	101	J00	11C	5 1 X 3 4 C	7 0 2 0 0 X	
		0426	Reversal (0106)	51X	101	J00	11C	5 1 X 3 4 C	7 0 2 0 0 X	
CAT-1	Online PIN	0106		51X	201	J10	14C	5 1 X 3 4 C	2 0 2 1 0 X	
		0206		51X	201	J10	14C	5 1 X 3 4 C	2 0 2 1 0 X	
		0226	Authorized	51X	201	J15	14C	5 1 X 3 4 C	2 0 2 1 5 X	
		0426	Reversal (0106)	51X	201	J15	14C	5 1 X 3 4 C	2 0 2 1 5 X	
	No CVM	0106		51X	201	J00	14C	5 1 X 3 4 C	2 0 2 0 0 X	
		0126	Offline Auth.	51X	201	J00	14C	5 1 X 3 4 C	2 0 2 0 0 X	
		0206		51X	201	J00	14C	5 1 X 3 4 C	2 0 2 0 0 X	
		0226	Authorized	51X	201	J00	14C	5 1 X 3 4 C	2 0 2 0 0 X	
		0226	Not authorized	51X	201	J00	14C	5 1 X 3 4 C	2 0 2 0 0 X	
CAT-2	No CVM	0106		50X	N01	J00	140	5 0 X 3 4 0	8 0 2 0 0 X	
		0126	Offline Auth.	50X	N01	J00	140	5 0 X 3 4 0	8 0 2 0 0 X	
		0206		50X	N01	J00	140	5 0 X 3 4 0	8 0 2 0 0 X	
		0226	Authorized	50X	N01	J00	140	5 0 X 3 4 0	8 0 2 0 0 X	
		0226	Not authorized	50X	N01	J00	140	5 0 X 3 4 0	8 0 2 0 0 X	
CAT-3	No CVM	0126	Offline Auth.	50X	O01	J00	110	5 0 X 3 4 0	9 0 2 0 0 X	
		0226	Not authorized	50X	O01	J00	110	5 0 X 3 4 0	9 0 2 0 0 X	
MSC (Fallback)										
Attended	Online PIN	0106		51X	101	M10	14C	5 1 X 3 4 C	1 0 7 1 0 X	
		0126	Error	51X	101	M10	11C	5 1 X 3 4 C	7 0 7 1 0 X	
		0206		51X	101	M10	14C	5 1 X 3 4 C	1 0 7 1 0 X	
		0226	Authorized	51X	101	M15	14C	5 1 X 3 4 C	1 0 7 1 5 X	
		0426	Reversal (0106)	51X	101	M15	14C	5 1 X 3 4 C	1 0 7 1 5 X	
	Signature	0106		51X	101	M50	14C	5 1 X 3 4 C	1 0 7 5 0 X	
		0106		51X	101	M50	11C	5 1 X 3 4 C	7 0 7 5 0 X	
		0126	Offline Auth.	51X	101	M50	14C	5 1 X 3 4 C	1 0 7 5 0 X	
		0206	(ICC Refund)	51X	101	M50	14C	5 1 X 3 4 C	1 0 7 5 0 X	
		0226	Authorized	51X	101	M54	14C	5 1 X 3 4 C	1 0 7 5 4 X	
		0226	Not authorized	51X	101	M54	11C	5 1 X 3 4 C	7 0 7 5 4 X	
		0426	Reversal (0106)	51X	101	M54	14C	5 1 X 3 4 C	1 0 7 5 4 X	
		0426	Reversal (0106)	51X	101	M54	11C	5 1 X 3 4 C	7 0 7 5 4 X	

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode
(continued)

				ISO 8583				APACS 60		
Environment	CVM	MTI	Transaction	POS Data Code				POS Capability Code, field 21:	POS Entry Mode, field 22:	
MSC (Fallback)										
Attended	No CVM	0106		51X	101	M00	14C	5 1 X 3 4 C	1 0 7 0 0 X	
		0126	Offline Auth.	51X	101	M00	14C	5 1 X 3 4 C	1 0 7 0 0 X	
		0206		51X	101	M00	14C	5 1 X 3 4 C	1 0 7 0 0 X	
		0226	Authorized	51X	101	M00	14C	5 1 X 3 4 C	1 0 7 0 0 X	
		0226	Not authorized	51X	101	M00	11C	5 1 X 3 4 C	7 0 7 0 0 X	
		0426	Reversal (0106)	51X	101	M00	11C	5 1 X 3 4 C	7 0 7 0 0 X	
CAT-1	Online PIN	0106		51X	201	M10	14C	5 1 X 3 4 C	2 0 7 1 0 X	
		0206		51X	201	M10	14C	5 1 X 3 4 C	2 0 7 1 0 X	
		0226	Authorized	51X	201	M15	14C	5 1 X 3 4 C	2 0 7 1 5 X	
		0426	Reversal (0106)	51X	201	M15	14C	5 1 X 3 4 C	2 0 7 1 5 X	
	No CVM	0106		51X	201	M00	14C	5 1 X 3 4 C	2 0 7 0 0 X	
		0126	Offline Auth.	51X	201	M00	14C	5 1 X 3 4 C	2 0 7 0 0 X	
		0206		51X	201	M00	14C	5 1 X 3 4 C	2 0 7 0 0 X	
		0226	Authorized	51X	201	M00	14C	5 1 X 3 4 C	2 0 7 0 0 X	
		0226	Not authorized	51X	201	M00	14C	5 1 X 3 4 C	2 0 7 0 0 X	
CAT-2	No CVM	0106		50X	N01	M00	140	5 0 X 3 4 0	8 0 7 0 0 X	
		0126	Offline Auth.	50X	N01	M00	140	5 0 X 3 4 0	8 0 7 0 0 X	
		0206		50X	N01	M00	140	5 0 X 3 4 0	8 0 7 0 0 X	
		0226	Authorized	50X	N01	M00	140	5 0 X 3 4 0	8 0 7 0 0 X	
		0226	Not authorized	50X	N01	M00	140	5 0 X 3 4 0	8 0 7 0 0 X	
CAT-3	No CVM	0126	Offline Auth.	50X	O01	M00	110	5 0 X 3 4 0	9 0 7 0 0 X	
		0226	Not authorized	50X	O01	M00	110	5 0 X 3 4 0	9 0 7 0 0 X	
Key Entered										
Attended	Signature	0106		51X	101	650	14C	5 1 X 3 4 C	1 0 6 5 0 X	
		0106		51X	101	650	11C	5 1 X 3 1 C	7 0 6 5 0 X	
		0126	Offline Auth.	51X	101	650	14C	5 1 X 3 4 C	1 0 6 5 0 X	
		0206	(Refund)	51X	101	650	14C	5 1 X 3 4 C	1 0 6 5 0 X	
		0226	Authorized	51X	101	654	14C	5 1 X 3 4 C	1 0 6 5 4 X	
		0226	Not authorized	51X	101	654	11C	5 1 X 3 1 C	7 0 6 5 4 X	
		0426	Reversal (0106)	51X	101	654	14C	5 1 X 3 4 C	1 0 6 5 4 X	
		0426	Reversal (0106)	51X	101	654	11C	5 1 X 3 1 C	7 0 6 5 4 X	
	No CVM	0126	Offline Auth.	51X	101	600	14C	5 1 X 3 4 C	1 0 6 0 0 X	
	No CVM Post Registration (Card not present)	0126	Offline error	51X	110	600	11C	5 1 X 3 1 C	7 1 6 0 0 X	
		0126	Online error	51X	110	600	11C	5 1 X 3 4 C	1 1 6 0 0 X	
		0206	Online	51X	110	600	14C	5 1 X 3 4 C	1 1 6 0 0 X	
		0226	Authorized	51X	110	600	11C	5 1 X 3 1 C	7 1 6 0 0 X	

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode
(continued)

				ISO 8583				APACS 60											
Environment	CVM	MTI	Transaction	POS Data Code				POS Capabil- ity Code, field 21:	POS Entry Mode, field 22:										
Contactless (ICC)																			
Attended	Online PIN	0106		51X	101	Z10	34C	5	1	X	3	4	C	1	0	3	1	0	X
		0126	Error	51X	101	Z10	11C	5	1	X	3	4	C	7	0	3	1	0	X
		0226	Authorized	51X	101	Z15	34C	5	1	X	3	4	C	1	0	3	1	5	X
		0426	Reversal (0106)	51X	101	Z10	34C	5	1	X	3	4	C	1	0	3	1	0	X
	Signature	0106		51X	101	Z50	34C	5	1	X	3	4	C	1	0	3	5	0	X
		0126	Error	51X	101	Z50	11C	5	1	X	3	4	C	7	0	3	5	0	X
		0206	Refund	51X	101	Z50	34C	5	1	X	3	4	C	1	0	3	5	0	X
		0226	Authorized	51X	101	Z54	34C	5	1	X	3	4	C	1	0	3	5	4	X
		0226	Not authorized	51X	101	Z54	11C	5	1	X	3	4	C	7	0	3	5	4	X
		0426	Reversal (0106)	51X	101	Z50	34C	5	1	X	3	4	C	1	0	3	5	0	X
	No CVM (Card present)	0106		51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	0	0	X
		0126	Error	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	0	0	X
		0226	Authorized	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	0	0	X
		0226	Not authorized	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	0	0	X
		0426	Reversal (0106)	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	0	0	X
	On Device/ Consumer Device	0106		51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	8	6	X
		0126	Error	51X	101	Z00	11C	5	1	X	3	4	C	1	0	3	8	6	X
		0226	Authorized	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	8	6	X
		0226	Not authorized	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	8	6	X
		0426	Reversal (0106)	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	8	6	X
Attended (no PIN Pad)	No CVM (Card present)	0106		51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	0	0	X
		0126	Offline Auth.	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	0	0	X
		0226	Authorized	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	0	0	X
		0226	Not authorized	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	0	0	X
		0426	Reversal (0106)	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	0	0	X
	On Device/ Consumer Device	0106		51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	8	6	X
		0126	Error	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	8	6	X
		0226	Authorized	51X	101	Z00	34C	5	1	X	3	4	C	1	0	3	8	6	X
		0226	Not authorized	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	8	6	X
		0426	Reversal (0106)	51X	101	Z00	11C	5	1	X	3	4	C	7	0	3	8	6	X

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode
(continued)

Environment	CVM	MTI	Transaction	ISO 8583				APACS 60	
				POS Data Code				POS Capabil- ity Code, field 21:	POS Entry Mode, field 22:
CAT-1	Online PIN	0106		51X	201	Z10	34C	5 1 X 3 4 C	2 0 3 1 0 X
		0126	Error	51X	201	Z10	11C	5 1 X 3 4 C	2 0 3 1 0 X
		0226	Authorized	51X	201	Z15	34C	5 1 X 3 4 C	2 0 3 1 5 X
		0426	Reversal (0106)	51X	201	Z10	34C	5 1 X 3 4 C	2 0 3 1 0 X
	No CVM	0106		51X	201	Z00	34C	5 1 X 3 4 C	2 0 3 0 0 X
		0126	Error	51X	201	Z00	11C	5 1 X 3 4 C	2 0 3 0 0 X
		0226	Authorized	51X	201	Z00	34C	5 1 X 3 4 C	2 0 3 0 0 X
		0226	Not authorized	51X	201	Z00	34C	5 1 X 3 4 C	2 0 3 0 0 X
	On Device / Consumer Device	0106		51X	201	Z00	34C	5 1 X 3 4 C	2 0 3 8 6 X
		0126	Error	51X	201	Z00	11C	5 1 X 3 4 C	2 0 3 8 6 X
		0226	Not Authorized	51X	201	Z00	34C	5 1 X 3 4 C	2 0 3 8 6 X
		0426	Reversal (0106)	51X	201	Z00	34C	5 1 X 3 4 C	2 0 3 8 6 X
CAT-2	No CVM	0106		50X	N01	Z00	340	5 0 X 3 4 0	8 0 3 0 0 X
		0126	Error	50X	N01	Z00	140	5 0 X 3 4 0	8 0 3 0 0 X
		0226	Authorized	50X	N01	Z00	340	5 0 X 3 4 0	8 0 3 0 0 X
		0226	Not authorized	50X	N01	Z00	340	5 0 X 3 4 0	8 0 3 0 0 X
	On Device / Consumer Device	0106		51X	N01	Z00	340	5 0 X 3 4 0	8 0 3 8 6 X
		0126	Error	51X	N01	Z00	140	5 0 X 3 4 0	8 0 3 8 6 X
		0226	Not Authorized	51X	N01	Z00	340	5 0 X 3 4 0	8 0 3 8 6 X
		0426	Reversal (0106)	51X	N01	Z00	340	5 0 X 3 4 0	8 0 3 8 6 X
CAT-3	No CVM	0126	Error	50X	O01	Z00	110	5 0 X 3 4 0	9 0 3 0 0 X
		0226	Not authorized	50X	O01	Z00	110	5 0 X 3 4 0	9 0 3 0 0 X
	On Device / Consumer Device	0126	Offline Auth.	50X	O01	Z00	110	5 0 X 3 4 0	9 0 3 8 6 X
		0226	Not authorized	50X	O01	Z00	110	5 0 X 3 4 0	9 0 3 8 6 X
Contactless (MSD)									
Attended	PIN	0126	Error	51X	101	A10	11C	5 1 X 3 4 C	7 0 4 1 0 X
		0206		51X	101	A10	14C	5 1 X 3 4 C	1 0 4 1 0 X
		0426	Reversal (0206)	51X	101	A10	14C	5 1 X 3 4 C	1 0 4 1 0 X
	Signature	0126	Error	51X	101	A50	14C	5 1 X 3 4 C	1 0 4 5 0 X
		0206		51X	101	A50	14C	5 1 X 3 4 C	1 0 4 5 0 X
		0226	Not Authorized	51X	101	A54	11C	5 1 X 3 4 C	7 0 4 5 4 X
		0426	Reversal (0206)	51X	101	A50	14C	5 1 X 3 4 C	1 0 4 5 0 X
	No CVM	0126	Error	51X	101	A00	11C	5 1 X 3 4 C	1 0 4 0 0 X
		0206		51X	101	A00	14C	5 1 X 3 4 C	1 0 4 0 0 X
		0226	Not Authorized	51X	101	A00	11C	5 1 X 3 4 C	7 0 4 0 0 X
		0426	Reversal (206)	51X	101	A00	14C	5 1 X 3 4 C	7 0 4 0 0 X

Table 2-13.94 - Valid Values for POS Capability Code and POS Entry Mode
(concluded)

				ISO 8583				APACS 60			
Environment	CVM	MTI	Transaction	POS Data Code				POS Capability Code, field 21:	POS Entry Mode, field 22:		
CAT-1	PIN	0126	Error	51X	201	A10	11C	5 1 X 3 4 C	2 0 4 1 0 X		
		0206		51X	201	A10	14C	5 1 X 3 4 C	2 0 4 1 0 X		
		0426	Reversal (0206)	51X	201	A10	14C	5 1 X 3 4 C	2 0 4 1 0 X		
	No CVM	0126	Error	51X	201	A00	11C	5 1 X 3 4 C	2 0 4 0 0 X		
		0206		51X	201	A00	14C	5 1 X 3 4 C	2 0 4 0 0 X		
		0226	Not Authorized	51X	201	A00	11C	5 1 X 3 4 C	2 0 4 0 0 X		
		0426	Reversal (206)	51X	201	A00	14C	5 1 X 3 4 C	2 0 4 0 0 X		
	CAT-2	No CVM	0126	Error	50X	N01	A00	110	5 0 X 3 4 0	8 0 4 0 0 X	
0206				50X	N01	A00	140	5 0 X 3 4 0	8 0 4 0 0 X		
0226			Not Authorized	50X	N01	A00	140	5 0 X 3 4 0	8 0 4 0 0 X		
0426			Reversal (206)	50X	N01	A00	140	5 0 X 3 4 0	8 0 4 0 0 X		
CAT-3	No CVM	0126	Error	50X	O01	A00	110	5 0 X 3 4 0	9 0 4 0 0 X		
		0226	Not Authorized	50X	O01	A00	110	5 0 X 3 4 0	9 0 4 0 0 X		

Legend: X = don't care.
 Reversal Advices (MTI = 0426) are mapped according to the rules defined for Original messages.
 Authorization Advices (MTI = 0126) are mapped primarily according to the rules defined for 0106 messages, alternatively according to specific 0126 messages.
 Supplementary Authorization: For MTI = 0106 where the Function Code = 107 (Supplementary Authorization. Amount estimated) the POS Data Code is *always* set to 510 101 650 14C (Key Entered & Signature) independent of the card technology and CVM indicated in the APACS message.
 NOTE: POS Entry Mode: Positions 4 and 5 are controlled by the PSAM. The PSAM will set the correct values in these positions before the POS Entry Mode is conveyed in the APACS message to the host (field 22). Furthermore, as the terminal is not capable of indicating in a Financial Advice whether the transaction has been authorized previously or not, the PSAM will alter the value of position 1 to 7 when not authorized.

2-13.9.6 Coding of Field 24 (Function Code)

The following table defines the applicable values for this system.

Table 2-13.95 - Applicable values for Field 24 (Function Code)

Value	Description
100–199	Used for message types 01XX
100	Original/Extended authorization. Amount accurate
101	Original/Extended authorization. Amount estimated
106	Supplementary authorization. Amount accurate
107	Supplementary authorization. Amount estimated

Table 2-13.96 - Applicable values for Field 24 (Function Code)
(continued)

Value	Description
200-299	Used for message types (01XX) and 02XX
200	Original financial request/advice
201	Previously approved authorization. Amount same
202	Previously approved authorization. Amount differs
300-399	Used for message types 03XX
300	Unassigned
380	Reconciliation report
400-499	Used for message types 04XX
400	Full reversal. Transaction did not complete as approved
401	Partial reversal. Transaction did not complete for full amount
600-699	Used for message types 06XX
680	Addendum record
690	Service record (Updates)
691	Service record (Internal PSAM validation)
800-899	Used for message types 08XX
851	Exchange control, give token
852	Clock synchronization
880	Installation
882	Advice transfer
884	PSAM update
886	PSAM deactivation
888	Generate reconciliation
889	Reconciliation report
890	Exchange control, Recon. report

2-13.9.7 Coding of Field 25 (Message Reason Code)

The following table defines the applicable values for this system.

Table 2-13.97 - Applicable values for Field 25 (Message Reason Code)

Value	Description
1000–1499	Reason for an advice message rather than a request message
1000	Not available
1003	Acquirer unavailable
1004	CAD (PSAM) processed
1005	ICC processing
1006	Under floor limit
1008	Acquirer timed out on original request
1010	Black list match
1011	ICC decline
1151	Backup message (from the Merchant Application Log in case of Data Store failure)
1156	Tearing/card has been withdrawn
1157	Card balance decreased
1500–1999	Reason for a request message rather than an advice message
1502	ICC random selection
1503	CAD (PSAM) random selection
1505	Online forced by ICC
1506	Online forced by card acceptor
1508	Online forced by CAD (PSAM)
1509	Online forced by issuer
1510	Over floor limit
1511	Merchant suspicious
4000–4999	Reason for a reversal
4000	Customer cancellation
4001	Unspecified, no action taken
4003	Format error, no action taken
4005	Original amount incorrect (Cancellation)
4007	CAD (PSAM) unable to complete transaction
4021	Time-out waiting for response
4204	ICC decline
6000–6999	Reason for an administrative advice
6000	Hotel
6001	Airlines
6002	Car rental
8000–8999	Reason for a network message
8600	Generate Consolidated Reconciliation
8601	Generate Turnover since Reconciliation

NOTE: The value 1151 is used for storing backup versions of advices in the Merchant Application.

2-13.9.8 Coding of Field 27 (Download Control)

This 6-character field consists of two sub-fields. Position 1 describes the required action and position 2-6 is a message number (starting with 00001). The message number in case of a repeat shall be the message number of the original message.

The following table defines the applicable values for position 1 for this system.

Table 2-13.98 - Applicable values for Field 27 (Download Control), position 1

Value	Description
1	Acknowledgement required
3	Positive acknowledgement
7	Negative acknowledgement, repeat requested
8	Negative acknowledgement, no repeat

2-13.9.9 Coding of Field 39 (Action Code)

This 4-digit field consists of three individually coded sub-fields.

The following tables define the applicable values for this system.

Position 1 defines the immediate action to take.

Table 2-13.99 - Applicable values for Field 39 (Action Code), position 1

Value	Description
0	Approved/accepted
1	Declined/rejected
2	Declined/pickup
3	Declined/merchant override
4	Refer
5	Failed, retry
6	Failed, no retry
8	National Use, see table 2-5.6 on page 2-5-125

Position 2 defines any subsequent action to take.

Table 2-13.100 - Applicable values for Field 39 (Action Code), position 2

Value	Description
0	No subsequent action
1	Hold connection – send message
2	Hold connection – receive message
3	Initiate new connection – immediately
4	Initiate new connection – deferred

Table 2-13.101 - Action Codes - Applicable Values

Value	ASW	Description	Source	
			Host	PSAM
0000	'0000'	No further details	II	
0001	'12BA'	Honour with identification	II	
0002	'12BB'	Approved for partial amount	II	
0003	'1010'	Approved (VIP)	II	
0007	'1011'	Approved, update ICC	II	
0060	'1012'	Account service–limit–alarm (National use)	II	
0061	'1013'	Card service–limit–alarm (National use)	II	
0062	'12F0'	Loyalty card – approved (National use)	II	
0063	'1014'	Approved but suspected fraud (National use)	II	
0064	'1015'	Approved without financial impact (National use)	II	
0065	'1016'	Approved but not authorized by issuer (National use)	(II)	II
1000	'1200'	No further details	II	
1001	'1240'	Expired card	II	
1002	'1270'	Suspected fraud	II	
1003	'12B0'	Card acceptor contact acquirer	II	
1004	'1201'	Restricted card	II	
1005	'12B1'	Card acceptor call acquirer's security department	II	
1006	'12C0'	Allowable PIN tries exceeded	II	
1007	'12B2'	Refer to card issuer	II	
1008	'12B3'	Refer to card issuer's special conditions	II	
1009	'12D0'	Invalid merchant	II	
1010	'1250'	Invalid amount	II	
1011	'12E0'	Invalid card number	II	
1112	'1220'	PIN data required	II	
1013	'12B4'	Unacceptable fee	II	
1014	'12B5'	No account of type requested	II	
1015	'12A4'	Requested function not supported	II	
1016	'12B7'	Not sufficient funds	II	
1017/1117	'1221'	Incorrect PIN	II	
1018	'12E1'	No card record	II	
1019	'1310'	Transaction not permitted to cardholder	II	
1020	'1311'	Transaction not permitted to terminal	II	
1021	'1260'	Exceeds withdrawal amount limit	II	
1022	'12B8'	Security violation	II	
1023	'1290'	Exceeds withdrawal frequency limit	II	
1024	'1312'	Violation of law	II	
1025	'1232'	Card not effective	II	

Table 2-13.101 - Action Codes - Applicable Values (*continued*)

Value	ASW	Description	Source	
			Host	PSAM
1026	'1280'	Invalid PIN block	II	II
1027	'1281'	PIN length error	II	II
1028	'1282'	PIN key synchronization error	II	
1029	'1271'	Suspected counterfeit card	II	
1060	'12B9'	Invalid date (National use)	II	
1061	'1203'	RFU (National use)	II	
1062	'120C'	Unable to locate previous message (National use)	II	
1063	'120D'	Data are inconsistent with original data (National use)	II	
1064	'1230'	Card entry found, but below low-range (National use)	II	
1065	'1231'	PAN-length not according to table-entry (National use)	II	
1066	'1202'	Cancellation cannot be accepted (National use)	II	
1067	'1300'	Match on previous transaction (National use)	II	
2000	'1500'	No further details (Pick up)	II	
2001	'1501'	Expired card (Pick up)	II	
2002	'1502'	Suspected fraud (Pick up)	II	
2003	'1503'	Card acceptor contact acquirer (Pick up)	II	
2004	'1504'	Restricted card (Pick up)	II	
2005	'1505'	Card acceptor call acquirer's security department (Pick up)	II	
2006	'1506'	Allowable PIN tries exceeded (Pick up)	II	
2007	'1507'	Special conditions (Pick up)	II	
2008	'1508'	Lost card (Pick up)	II	
2009	'1509'	Stolen card (Pick up)	II	
2010	'150A'	Suspected counterfeit card (Pick up)	II	
5000	'1618'	No host response received		II
5303	'1601'	Re-enter transaction	II	II
5304	'1602'	Format error	II	II
5316	'160C'	MAC incorrect	II	II
5406	'1603/ '1020/ '1618'	Cut-over in process	II	
5407	'1604/ '1020'	Card issuer or switch inoperative	II	
5408	'1605'	Transaction destination cannot be found for routing	II	
5409	'1606'	System malfunction	II	
5410	'1607/ '1020'	Card issuer signed off	II	
5411	'1608/ '1020'	Card issuer timed out	II	

Table 2-13.101 - Action Codes - Applicable Values (*concluded*)

Value	ASW	Description	Source	
			Host	PSAM
5412	'1609'/ '1020'	Card issuer unavailable	II	
5414	'160A'	Not able to trace back to original transaction	II	
5415	'160B'/ '1020'	Reconciliation cut-over or checkpoint error	II	
5417	'160D'	MAC key synchronization error	II	
5418	'160E'	No communication keys available for use	II	
5419	'160F'	Encryption key synchronization error	II	
5420	'1611'	Security software/hardware error – try again	II	
5421	'1612'	Security software/hardware error – no action	II	
5423	'1613'	Request in progress	II	
5445	'1614'/ '1020'	Host time-out (Private use)	II	
5484	'1615'	No valid conversion for a field value (National use)	II	
6002	'1780'	Invalid transaction	II	
6005	'1770'	Acquirer not supported by switch	II	
6013	'17A0'	Duplicate transmission	II	
6022	'17A1'	Message number out of sequence	II	
6050	'17A2'	Violation of business arrangement (National use)	II	
8000	–	Accepted/Successful	II	
8001	–	Accepted, unspecified mismatch in data	II	
8002	–	Accepted, format error (e.g. MAC error)	II	
8003	–	Accepted, card data mismatch	II	
8004	–	Accepted, merchant data mismatch	II	
8005	–	Accepted, PSAM ID mismatch	II	
8020	–	Rejected	II	
8421	–	Rejected, try again later	II	
8022	–	Rejected, format error (e.g. MAC error)	II	
8023	–	Rejected, card data mismatch	II	
8024	–	Rejected, merchant data mismatch	II	
8025	–	Rejected, PSAM ID mismatch	II	

2-13.9.10 TLV Coding of Field 44 (Additional Response Data)

This field is TLV coded according to the definition in section 2-13.9.1 page 2-13-65.

The applicable data objects are listed in the following table.

Table 2-13.102 - Applicable data objects for Field 44 (Additional Response Data)

Tag	Item	Attrib.	Value
A3	Card Reconciliation Counter ID	an3	Example of values are listed in table 2-13.103
A4	Card Reconciliation Counter Name	ans16	Example of values are listed in table 2-13.103
A5	Card Name (for printing)	ans16	Example of values are listed in table 2-13.104
BG	Acquirer Identification	..ans24	Text string specifying the Acquirer used
BH	Acquirer Merchant Number	..ans24	Text string, the customer(merchant) reference at the Acquirer
T1	Authorization Response Code	an2	See ref. 10: "ISO 8583:1987" & ref. 20: "EMV ICC Specification"
TY	Issuer Envelope Response Data	..b65	At the Issuer discretion

Table 2-13.103 - Example of Values for Reconciliation Identifiers and Names

Reconciliation Counter Id	Reconciliation Counter Name
001	DANKORT
002	DANSKE EC/MC
003	UDL.EC/MC/VI/JCB
004	AMERICAN EXPRESS
005	DINERS
006	D KORT BONUS
008	FORBRUGSFORENING
009	ACCEPTCARD
010	SPNKONTOKORT
011	EKSPRESKORT
012	SBVKONTOKORT
013	COMPUTERCITY
014	BG FINANS
015	IKANO FINANS
016	CASTROL CREDIT
019	BG BANK – TAXA

Table 2-13.104 - Example of Values for Card Names to Print

Card Name (for Printing)
ACCEPTCARD
AMERICAN EXPRESS
BG FINANS
CASTROLCREDIT
COMPUTERCITY
D KORT BONUS
DANKORT
DINERS
EKSPRESKORT
FBF 1886
IKANO FINANS
JCB
MAESTRO
SBVKONTOKORT
SPNKONTOKORT
VISA

2-13.9.11 TLV Coding of Field 46 (CAD Management/Service Quality Data)

This field is TLV coded according to the definition in section 2-13.9.1 page 2-13-65. Table 2-13.117 page 2-13-103 gives the relation between messages and applicable tags.

Table 2-13.105 - Applicable values for Field 46 (CAD Management/Service Quality Data)

Tag	Item	Attrib.	Length ²⁾	Value
T2	PIN Pad ID	b8	12	IDPPCREATOR □IDPP
T3	MAD-Handler ID	ans8	12	See below
T4	Terminal Capabilities	b3	7	See ref. 20: "EMV ICC Specification"
T5	Additional Terminal Capabilities	b5	9	See ref. 20: "EMV ICC Specification"
T6	Software Version Number	b2	6	At the discretion of the Terminal Supplier
T7	Hardware Version Number	b2	6	At the discretion of the Terminal Supplier
T9	Terminal Approval Number	b2	6	
TA	Terminal Type	b1	5	See ref. 20: "EMV ICC Specification"
TB	Info Level	b1	5	
TC	Update Results	..b99	..103	Generated by the PSAM
TD	Response time for previous on-line transaction ¹⁾	b18	22	Coded as PSAM identifier (13 bytes), STAN (3 bytes) and response times in milliseconds (2 bytes)

Table 2-13.105 - Applicable values for Field 46 (CAD Management/Service Quality Data) *concluded*

Tag	Item	Attrib.	Length ²⁾	Value
TE	Number of time-outs ¹⁾	n2	5	For APACS messages, including advices and administrative messages
TF	Number of card reader errors ¹⁾	n2	5	Including magnetic stripe card errors
TG	Number of unsupported cards ¹⁾	n2	5	
TH	Number of communication errors between CAD and Merchant Application ¹⁾	n2	5	
TI	Number of System Faults	b2	6	Generated by the PSAM
TJ	Number of Fatal Errors	b2	6	Generated by the PSAM
TK	Application Status Words – ASW1 ASW2	b2	6	Generated by the PSAM
TP	PSAM version	b2	6	Major and minor number
TQ	PSAM Life Cycle State	b1	5	
TR	PSAM Date	n6	7	YYMMDD
TS	Grand Total	b6	10	2 bytes total transaction counter succeeded by a 4 bytes total amount
9A	PTS Request Data	b33	37	Generated by PSAM, only in Request at PTS, see 2-15.2.116 for detailed definition
9B	PTS Response Data	b74/ b51	78/ 55	Only in response and when request contained Tag 9A. Size depends on MK _{PSAM} . See 2-15.2.117 for detailed information.
9C	PCI Data		var	From Terminal in response to <i>Install 2</i> command, see 2-15.2.102 for detailed information.
9D	PSAM Parameters	b14	18	Inserted by PSAM. Terminal and PSAM setting, see 2-15.2.112 for detailed information

Legend:

1) Candidates for the data element “Statistics”, which is part of the *Initiate Payment* command. At the discretion of the Terminal Supplier.

2) Length includes the total length of Tag, length and Value.

Examples:
Tag TF indicating 12 card reader errors: 54 46 00 01 12
Tag TD response time for previous transaction: 54 44 00 12 A0 00 00 01 20 00 00 00 05 03 95 6A 56 00 00 04 04 56

- 2-13.9.11.1 A Response time for previous transaction (Tag TD) shall state the elapsed time from the host request message is available (response to the *Payment* command or *Validate Data* command) to the corresponding host response is ready for validation (*Validate Data* command).

Coding of the MAD-Handler ID

This field uniquely identifies the terminal equipment (or more specifically, the MAD-Handler) as seen by the PSAM. The identifier consists of an 8-byte field subdivided as defined by table 2-13.106.

Table 2-13.106 - Coding of the MAD-Handler ID

Name	Attributes	Length	Remarks
Terminal Manufacturer Id.	ans3	3	Identifier assigned by Nets Denmark A/S
Terminal Serial Number	ans5	5	Individual MAD-Handler Id.

2-13.9.12 Coding of Field 47 (Additional Data - National)

This field is TLV coded according to the definition in section 2-13.9.1 page 2-13-65.

Table 2-13.107 - Applicable values for Field 47 (Additional Data - National)

Tag	Item	Attrib.	Value
BE	Token based transaction flag	n1	Only present in Financial and Reversal Advices. Is '1' when then the transaction was generated from a token, else it is '0'.
BF	Offline since	n10	Only present in offline generated Financial Advices. The content is the timetag from when the terminal went offline (first offline transaction, format YYMMDDhhmm)
TL	KEK _{PIN} Version	b1	
TM	[KSES _{PIN}]	b16	
TN	PIN Block Format	n1	Allowed values are 0, 1 and 2
V5	CV-2	an4 ¹⁾	Card verification data (for key entered transactions)
TX	Issuer Envelope Data	..b100 ²⁾	To be provided by the terminal using the <i>Set Debit/Credit Properties</i> command
Legend:			
1) = Pad with leading 'F' if number is a 3 digit value.			
2) = Maximum value for EMV transactions is for Nets PSAMs with a version below 70 limited to 60 bytes.			

2-13.9.13 Coding of Field 55 (ICC System Related Data)

This field contains IC Card related data both when sending messages from the terminal to the host and when receiving responses.

The TLV coding used conform to ref. 20: "EMV ICC Specification".

NOTE: This coding is different from the TLV coding defined for other fields in section 2-13.9.1 page 2-13-65.

Table 2-13.108 - Field 55 for Request and Advice Messages

Name	Tag	Attributes	Length ¹⁾	Remarks	
Application Identifier (AID)	M	'4F'	b5 – b16	7-18	
Application Expiration Date	M	'5F24'	n3	5	YYMMDD
Application Cryptogram	M	'9F26'	b8	11	ARQC/TC/AAC
Cryptogram Information Data	M	'9F27'	b1	4	
Issuer Application Data	C ²⁾	'9F10'	..b32	..35	
Unpredictable Number	C ³⁾	'9F37'	b4	7	
CVM Results	M	'9F34'	b3	6	
Application Transaction Counter (ATC)	M	'9F36'	b2	5	
Terminal Verification Result (TVR)	M	'95'	b5	7	
Transaction Date	M	'9A'	n6	5	YYMMDD. From DTHR in <i>Initiate Payment</i> command
Transaction Type	M	'9C'	n2	3	First two digits from field 3
Amount Authorized (numeric)	M	'9F02'	n12	9	Also present in field 4
Application Interchange Profile (AIP)	M	'82'	b2	4	
Terminal Country Code	M	'9F1A'	n3	5	
Amount, Other (numeric)	C ⁴⁾	'9F03'	n12	9	Also present in field 8
Terminal Capabilities	M	'9F33'	b3	6	
Transaction Status Information (TSI)	M	'9B'	b2	4	Audit purposes only
Authorization Response Code	C ⁵⁾	'8A'	an2	4	For cryptogram verification
Transaction Currency Code	M	'5F2A'	n3	5	Also present in field 49
Issuer Script Results	C ⁶⁾	'D0'	b5	7	Nets-defined Tag
Application Version Number	M	'9F09'	b2	5	Added from Finnish req.
Interface Device (IFD) Serial Number	M	'9F1E'	b8	11	Added from Finnish req.
Terminal Type	M	'9F35'	b1	4	Added from Finnish req.
Master Card TCC	M	'9F53'	b1	4	Added from Finnish req.
Transaction Sequence Counter	C	'9F41'	b4 – b8	7-11	Contactless
Form Factor Indicator	C ⁷⁾	'9F6E'	b4	7	Contactless
Customer Exclusive Data	C ⁷⁾	'9F7C'	..b32	..35	Contactless
Third Party Data/Device Type Indicator	C ⁸⁾	'9F6E'	b5 – b32	8-35	Contactless
Maximum number of bytes (contact)				179	
Maximum number of bytes (Contactless)				232/214	PayWave/PayPass

Table 2-13.108 Field 55 for Request and Advice Messages (*concluded*)

Legend:
M: Mandatory
C: Conditional
1) Length includes the total length of Tag, length and Value.
2) Present only if the Issuer apply Issuer Application Data.
3) Present only if the card requests the Unpredictable Number in CDOL1/CDOL2.
4) Present if Amount, Other is different from zero.
5) Omitted in case of an Authorization Request.
6) Present in the Financial Advice/Reversal Advice if Issuer Scripts has been provided in the previous Authorization Request.
7) Visa payWave (qVSDC) defined data elements.
8) MasterCard <i>PayPass</i> defined data elements.

Table 2-13.109 - Field 55 for Response Messages

Name	Tag	Attributes	Length ¹⁾	Remarks
Issuer Authentication Data	O	'91'	b8..b16	10..18
Issuer Script 1	O	'71'	..b127	..129
Issuer Script 2	O	'72'	..b127	..129
Legend:				
O: Optional				
1) Length includes the total length of Tag, length and Value.				

NOTE: The data elements listed in table 2-13.109 may be absent.

2-13.9.14 Coding of Field 56 (Original Data Elements)

This field uniquely identifies a previously performed Authorization Request, Financial Request or Financial Advice.

Table 2-13.110 - Field 56 (Original Data Elements)

Name	Attributes	Length	Remarks
MTI	an4	4	Message Type Identifier
Systems Trace Audit Number	n6	3	STAN
Time, local transaction	n6	3	Format: hhmmss
Date, local transaction	n4	2	Format: MMDD
RID _{PSAM}	b5	5	The entity assigning PSAM Creator Ids
ID _{PSAMCREATOR}	b4	4	The entity assigning PSAM Ids
ID _{PSAM}	b4	4	Individual PSAM Id

2-13.9.15 Coding of Field 59 (Additional Data Capture)

This field is used both in the direction to the Host and from the Host.

- 2-13.9.15.1 A Field 59 (Additional Data Capture) shall be coded according to table 2-13.111. The field shall be TLV coded according to the definition in section 2-13.9.1 page 2-13-65.

Table 2-13.111 - Field 59 (Additional Data Capture) from/to Host

Tag	Item	Direction ²⁾	Attrib.	Description
4N	Customer Reference Number	to Host	..an32	Value assigned by the merchant for identification of the actual transaction
4O	Receipt Number	to Host	..an10	Value assigned by the merchant and printed on the cardholders receipt for identification of the receipt/transaction.
4P	IFSF Field 48 ¹⁾	to Host	..bxx	Message Control Data containing additional data relevant/needed for the actual transaction.
4Q	IFSF Field 62 ¹⁾	to Terminal	..bxx	Product Data describing differences between the products requested and any restrictions
4R	IFSF Field 63 ¹⁾	to Host	..bxx	Product Data describing the products purchased by the actual request.
4T	VAT percentage and Product type	to Host	..bxx	One or more set of information on VAT percentage and corresponding product types.
4W	Entry – Exit Station	to Host	..bxx	Information on merchant and where the transaction was performed. May as well contain time information.
4Z	Supplier and Service Point	to Host	..bxx	Information on where the transaction was performed and the supplier behind the service.
6J	Term. Supplier ³⁾	to Host	..an2	Terminal supplier identifier as assigned by Finnish Certification authorities.
6K	Term. Type ³⁾	to Host	..an1	Terminal type identifier as assigned by Finnish Certification authorities.
6R	Paym. Terminal Type ³⁾	to Host	..an1	Payment Terminal type as defined for Finland. Range 1 – 5.
UQ	Finnish Payment Ref. Number ³⁾	to Host	..n20	A unique payment reference as defined for Finnish terminals.
Legend:				
1) = IFSF, International Forecourt Standards Forum, an ISO 8385:1993 based standard.				
2) = Direction indicates either towards the Host (from PSAM/Terminal) or towards the Terminal (from Host).				
3) = Only for Finnish Terminals				
Note:				
Data stored as T-L-V, i.e. 2 ASCII char Tag followed by 2 hex. byte Length and x byte Value (data).				

2-13.9.16 Coding of Field 60 (PSAM Identifier)

This field uniquely identifies a given PSAM.

- 2-13.9.16.1 A Field 60 (PSAM Identifier) shall be coded according to table 2-13.112.

Table 2-13.112 - Field 60 (PSAM Identifier)

Name	Attributes	Length	Remarks
RID _{PSAM}	b5	5	The entity assigning PSAM Creator Ids
ID _{PSAMCREATOR}	b4	4	The entity assigning PSAM Ids
ID _{PSAM}	b4	4	Individual PSAM Id

- 2-13.9.16.2 A As Field 60 is an LVAR field, the PSAM Identifier shall be preceded by a one-byte length field with the value '0D'.

2-13.9.17 Coding of Field 61 (Random Number)

This field contains a random number generated by the PSAM. It is sent enciphered to the Terminal Operator host where it is deciphered and returned to the Terminal in plaintext.

Field 61 (Random Number) will be coded as an 8-byte binary integer.

As Field 61 is an LVAR field, the Random Number will be preceded by a one-byte length field with the value '08'.

2-13.9.18 Coding of Field 62 (Merchant Initiative)

This field contain flags indicating whether the CVM and/or on-line/offline is forced by the merchant.

2-13.9.18.1 A Field 62 (Merchant Initiative) shall be coded on one byte according to table 2-15.17 page 2-15-25.

2-13.9.18.2 A As Field 62 is an LVAR field, the Merchant Initiative shall be preceded by a one-byte length field with the value '01'.

2-13.9.19 TLV Coding of Field 63 (PSAM Updates/Reconciliation Data)

This field is TLV coded according to the definition in section 2-13.9.1 page 2-13-65.

2-13.9.19.1 A If more data objects are present, the corresponding *PSAM Update* commands shall be sent in the order of presence in the message received from the Terminal Operator host.

See section 2-5.13.3 page 2-5-93.

Table 2-13.113 - Applicable values for Field 63 (PSAM Updates)

Tag	Item	Attrib.	Value
TO	PSAM Update	b..MAX	C-APDU to send to the PSAM
TW	Reconciliation Report Data	b..MAX	Consolidated Reconciliation/Turnover Report data

2-13.9.19.2 A As Field 63 is an LLVAR field, the PSAM Updates/Reconciliation Report Data shall be preceded by a two-bytes length field.

2-13.9.19.3 A Reconciliation Report Data, Tag TW, shall consists of blocks of 24 printable characters, according to ref: 12 "ISO 8859-15" each followed by NewLine, '0A'.

2-13.9.20 Coding of Field 71 (Message Number)

This 8-digit field indicates the number of addendum record(s) attached to a specific Financial Advice.

The four most significant digits indicates the segment number of this addendum record while the 4 least significant digits indicates the total number of segments.

2-13.9.21 TLV Coding of Field 72 (Addendum Record)

Addendum records are used to convey additional information concerning the payment transaction.

Tags for specific data elements are defined for the following merchant categories:

- Hotel/Lodging see table 2-13.114 page 2-13-95
- Airlines/Passenger Transport see table 2-13.115 page 2-13-97
- Car Rental/Vehicle Rental see table 2-13.116 page 2-13-100

Table 2-13.114 - Applicable values for Field 72 (Hotel/Lodging)

Tag	Item	Attrib.	Description	Value
H1	Customer-code	an17	A reference number provided by the cardholder to the merchant providing the goods or services.	Mandatory. If the cardholder does not provide a reference number, the field must be filled with spaces.
H2	Arrival date	n8	The day the cardholder arrived.	YYYYMMDD Mandatory.
H3	Departure date	n8	The day the cardholder checked out.	YYYYMMDD Mandatory.
H4	Folio number	an10	The number assigned to the lodging message.	Mandatory.
H5	Phone number	an12	The phone number used to identify specific property by its local phone number.	
H6	Service phone number	an12	A customer support phone number that can be used by the cardholder.	
H7	Daily rate	n12	The daily rental rate charged for the room.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
H8	Daily room tax	n12	The daily room tax that is charged to the cardholder. The room tax is a tax that may be charged by the hotel in addition to the daily room rate.	Same currency as 1240 presentment, field 49. Max. 9999999 (7 digits).
H9	Program code	an2	A code used to identify special circumstances, such as "frequent renter".	The field is optional (no special coding scheme is currently defined).
HA	Phone charges	n12	The amount charged to the cardholder for telephone calls made during his/her stay.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HB	Restaurant/room service	n12	The amount charged to the cardholder for hotel restaurant and room services during his/her stay.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HC	Bar/minibar charges	n12	The amount charged to the cardholder for hotel bar and minibar drinks during his/her stay.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HD	Gift shop charges	n12	The amount charged to the cardholder for purchases made at the gift shop during his/her stay.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HE	Laundry/dry clean charges	n12	The amount charged to the cardholder for laundry and dry cleaning services during his/her stay.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).

Tag	Item	Attrib.	Description	Value
HF	Total non-room charges	n12	The amount charged to the cardholder for total non-room services.	Same currency as 1240 presentment, field 49.
HG	Valet parking charges	n12	The amount charged to the cardholder for valet parking.	Same currency as 1240 presentment, field 49.
HH	Movie charges	n12	The amount charged to the cardholder for movies.	Same currency as 1240 presentment, field 49.
HI	Business center charges	n12	The amount charged to the cardholder for business center use.	Same currency as 1240 presentment, field 49.
HJ	Food/beverage charges	n12	The amount charged to the cardholder for food/beverage.	Same currency as 1240 presentment, field 49.
HK	Health club charges	n12	The amount charged to the cardholder for health club use.	Same currency as 1240 presentment, field 49.
HL	Folio cash advances	n12	The amount of folio cash advances.	Same currency as 1240 presentment, field 49.
HM	No-show indicator	an1	This field can be used to indicate that the transaction was due to a no-show charge.	0 = not applicable 1 = no-show.
HN	Lodging extra charges	n6	Type of additional extra charges added to a customer's bill after checkout.	Each position of the field can be used to indicate a type of charge. If there are less than 6 charges they must be left-justified, space-filled or zero-filled to the right. The following are the lodging extra charge codes: Space = No extra charges 0 = No extra charges 2 = Restaurant 4 = Gift shop 5 = Telephone 6 = Other 7 = Laundry
HO	Other service codes	an3	A code that specifies the type of additional charges to be paid by the cardholder.	If a value is provided, it must be left justified and filled with trailing spaces.
HP	Other charges	n12	Charges related to service for which a specific field has not been defined in the 1644 message.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HQ	Billing adjustment amount	n12	The adjusted billing amount added after the cardholder checked out.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HR	Number of days	n2	Room nights.	
HS	Total room tax	n12	Total room tax amount.	Same currency as 1240 presentment, field 49.

Tag	Item	Attrib.	Description	Value
HT	Total tax	n12	Total tax amount.	Same currency as 1240 presentment, field 49.
HU	Prepaid expenses	n12	Prepaid expenses amount.	Same currency as 1240 presentment, field 49.
HV	Record number	n4	Sequence of lodging addendum record associated with the same presentment.	Max. 99. Mandatory.
HX	Tot-records	n4	Total lodging addendum's associated with same presentment.	Max. 99. Mandatory.

Table 2-13.115 - Applicable values for Field 72 (Airlines/Passenger Transport)

Tag	Item	Attrib.	Description	Value
H1	Customer-code	an17	The cost center code assigned by the corporation. The employee who purchases goods/services on account of his/her corporation will quote the customer code to the ME.	
I1	Person-name	an40	Name of person to whom ticket was issued or cardholder's name.	Mandatory.
IM	No-of-passengers	n3	Number of passengers.	
IN	Employee-no	an15	Employee's number.	
IO	Travel-agency-code	an8	The code (IATA number) of the travel agency that issued the ticket.	Mandatory.
IP	Travel-agency-name	an25	Name of the travel agency that issued the ticket.	
IQ	Ticket-no	an14	Number of the travel ticket, including the check digit.	Mandatory.
I4	Return-date	n8	Return day.	YYYYMMDD
IR	From-airport	an20	Code identifying departure airport or city.	4 blocks of 5 characters each, e.g. 'AAL CPH ARN' Leg 1 = departure airport AAL Leg 2 = departure airport CPH Leg 3 = departure airport ARN The first block of the first passenger transport addendum related to a 1240 presentment is the first airport of the journey. Mandatory.

Tag	Item	Attrib.	Description	Value
IS	Carrier-code	an8	Code identifying the carrier.	4 blocks of 2 characters each. One block for each leg of the flight beginning with leg 1. Mandatory.
IT	Service-class	an8	Travel class code.	4 blocks of 2 characters each. One block for each leg of the flight beginning with leg 1.
IU	Stop-over-code	an4	Stop over code.	4 blocks of 1 character each. One block for each leg of the flight beginning with leg 1. Values for each block: Spaces or O = Stopover allowed X = Stopover not allowed.
IV	Destination-airport	an20	Code identifying destination airport or city.	4 blocks of 5 characters each. One block for each leg of the flight beginning with leg 1. E.g. 'AAL CPH ARN' Leg 1 = departure airport AAL Leg 2 = departure airport CPH Leg 3 = departure airport ARN Mandatory.
IX	Fare-basis-code	an32	Code associated with the ticket price charged by the airline company.	4 blocks of 8 characters each. One for each leg of the flight. In case of a direct flight, there is just one fare basis code. In case of a flight with stopovers, there will be as many fare basis codes as there are trip legs.
IY	Coupon-no	n4	Coupon number.	4 blocks of 1 character each. One for each leg of the flight. Valid values for each block are 1, 2, 3, 4 and space.
IZ	Flight-no	an20	Flight number.	4 blocks of 5 characters each. One for each leg of the flight.
J1	Departure-date	an24	Departure date.	4 blocks of 6 characters each. One for each leg of the flight. YYMMDD If not available, use transaction date.

Tag	Item	Attrib.	Description	Value
J2	Departure-time	n16	Departure time.	4 blocks of 4 characters each. One for each leg of the flight. HHMM
J3	Arrival-time	n16	Arrival time.	4 blocks of 4 characters each. One for each leg of the flight. HHMM
J4	Turn-around-point	an5	Point of turnaround.	
J5	Turn-around-text	an30	Turnaround text.	
J6	Restricted-ticket-indic	an1	If ticket is refundable or not.	Space or 0 = not restricted 1 = restricted (non refundable ticket)
J7	Computer-reserv-system	an4	Code for computer system.	Spaces or one of the following codes: "STRT" = Start "PARS" = TWA "DATS" = Delta "SABR" = Sabre "DALA" = Covia-apollo "BLAN" = Dr. Blank "DERD" = DER "TUID" = TUI
J8	Total-fare-amount	n12	Total fare amount.	Same currency as 1240 presentment, field 49.
HT	Total-tax	n12	Total tax amount.	Same currency as 1240 presentment, field 49.
J9	National-tax-amount	n12	National tax amount.	Same currency as 1240 presentment, field 49.
JA	Total-fee-amount	n12	Total fee amount.	Same currency as 1240 presentment, field 49.
JB	Exchange-ticket-no	an13	Exchange ticket number.	Left justified.
JC	Exchange-ticket-amount	n12	Exchange ticket amount.	Same currency as 1240 presentment, field 49.
JD	Internet-indicator	an1	Internet indicator.	Spaces or "Y" = Yes "N" = No
JE	Article-no	an10	Article number from bureau. Used for car rental/hotels etc.	
JF	Article-text	an30	Article name from bureau.	

Tag	Item	Attrib.	Description	Value
JG	Ticket-issuer-country	an40	The country where the ticket was issued.	
HV	Record-number	n4	Sequence of passenger addendum records associated with the same presentment.	Max. 99 Mandatory.
HX	Tot-records	n4	Total passenger addendum records associated with the same presentment.	Max. 99 Mandatory.

Table 2-13.116 - Applicable values for Field 72 (Car Rental/Vehicle Rental)

Tag	Item	Attrib.	Description	Value
H1	Customer-code	an17	The cost center code assigned by the corporation. The employee who purchases goods/services on account of his/her corporation will quote the customer code to the ME.	
HY	Corporate ID	an12		
HZ	Rental agreement number	an9	The reference number of the original car rental invoice or contract.	Mandatory.
I1	Person name	an40	Name of person renting the vehicle.	Mandatory.
I2	Rental return city	an25	Name of city where vehicle was returned.	Mandatory.
I3	Rental return state/country	an3	ISO code for the state or country where the vehicle was returned.	
I4	Return date	n8	The day the car was returned.	YYYYMMDD
I5	Checkout-date	n8	The day the car was picked up.	YYYYMMDD
I6	Return location id	an10	Code, address or phone number used to identify the location where the vehicle was returned.	Mandatory.
H6	Service phone number	an12	Customer support number that can be used by the cardholder.	Mandatory.
I7	Rental class	an4	Classification of the car that was rented.	
I8	maximum free miles/km	n4	The number of free miles/km granted to the customer for the duration of the agreement.	

Tag	Item	Attrib.	Description	Value
I9	Adjusted amount indicator	an1	An indicator specifying if any miscellaneous charges were incurred after the vehicle was returned.	Space or “A” = Drop of charges “B” = Delivery charges “C” = Parking expenses “D” = Extra hours “E” = Violations “X” = More than one of the above.
IA	Adjusted amount	n12	The amount charged in addition to the vehicle rental agreement, after the vehicle was returned.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
H9	Program code	an2	Used to identify special circumstances such as frequent renter.	Left justified filled with spaces.
HR	Number of days	n2	The number of days the car was rented.	
H7	Daily rate	n12	Daily rental charge for the vehicle.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
IB	Weekly rental rate	n12	Weekly rental charge for the vehicle.	Same currency as 1240 presentment, field 49.
IC	Mile/km indicator	an1	An indicator specifying if the unit of distance is miles or km.	“m” or “k”.
ID	Total miles/km	n4	The total number of miles/km driven by the customer.	
JG	Rate per unit	n12	The rate charged for each mile/km.	Same currency as 1240 presentment, field 49. Max 999999 (6 digits).
IE	Auto towing	n12	The amount charged for auto towing.	Same currency as 1240 presentment, field 49.
IF	Extra mileage charges	n12	The amount charged for extra mileage.	Same currency as 1240 presentment, field 49.
IG	Late return charges	n12	The amount charged for “late return”.	Same currency as 1240 presentment, field 49.
IH	Fuel charges	n12	The amount charged for fuel.	Same currency as 1240 presentment, field 49.
II	One way drop off charges	n12	The amount charged for “one way drop off”.	Same currency as 1240 presentment, field 49.
IJ	Insurance charges	n12	The amount charged for the rental insurance purchased by the customer.	Same currency as 1240 presentment, field 49. Max. 999999999 (9 digits).
HA	Phone charges	n12	The amount charged for telephone calls.	Same currency as 1240 presentment, field 49.

Tag	Item	Attrib.	Description	Value
IK	Car rental extra charges	n6	Valid car rental extra codes.	0 = No extra charges 1 = Gas 2 = Extra mileage 3 = Late return 4 = One way service fee 5 = Parking violation
HT	Total tax	n12	Total tax amount.	Same currency as 1240 presentment, field 49.
HM	No show indicator	an1	Used to indicate that the transaction is due to a no-show charge.	0 = not applicable 1 = no-show for specialized vehicle.
HV	Record number	n4	Addendum sequence. Sequence of vehicle addendum record associated with the same presentment.	Max. 99 Mandatory.
HX	Tot-records	n4	Total vehicle rental addendum's associated with the same presentment.	Max. 99 Mandatory.

Table 2-13.117 - Field 46 - Messages and related Tags

Tag	Message Type	Auth. Req		Auth. Adv.		Finan. Req.		Finan. Adv.		File Action		Rev. Adv.		Addendum		Service Rec.	
		Function Code										680		690			
		0106	0116	0126	0136	0206	0216	0226	0236	0360	0370	0426	0436	0624	0634	0624	0634
T2	PIN Pad ID	C ¹⁾		O		C ¹⁾											
T3	MAD-Handler ID	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
T4	Terminal Capabilities																
T5	Additional Terminal Capabilities																
T6	Software Version Number																
T7	Hardware Version Number																
T9	Terminal Approval Number	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
TA	Terminal Type																
TB	Info Level																
TC	Update Results																M
TD	Response time for previous transaction	O		O		O		O									
TE	Number of time-outs	O		O		O		O									
TF	Number of card reader errors	O		O		O		O									
TG	Number of unsupported cards	O		O		O		O									
TH	Number of communication errors between CAD and Merchant Application	O		O		O		O									
TI	Number of System Faults	O		O		O		O				O		O		O	
TJ	Number of Fatal Errors	O		O		O		O				O		O		O	
TK	Application Status Words			M								M					
TP	PSAM version	M		M		M		M				M		M		M	
TQ	PSAM Life Cycle State	O		O		O		O				O		O		O	
TR	PSAM Date	O		O		O		O				O		O		O	
TS	Grand Total	M		M		M		M				M					

Legend: M = Mandatory, O = Optional, C¹⁾ = if CVM = PIN

Table 2-13.117 - Field 46 - Messages and related Tags (concluded)

Tag	Message Type	Clock Sync		Installation		Advice Transfer		PSAM Update Req.		Exch .	PSAM Deactivate	
		852		880		882		884		851	886	
		0804	0814	0804	0814	0804	0814	0804	0814	0844	0804	0814
T2	PIN Pad ID											
T3	MAD-Handler ID	M	M	M	M	M	M	M	M	M	M	M
T4	Terminal Capabilities			M								
T5	Additional Terminal Capabilities			M								
T6	Software Version Number			M								
T7	Hardware Version Number			M								
T9	Terminal Approval Number	M	M	M	M	M	M	M	M	M	M	M
TA	Terminal Type			M								
TB	Info Level			M								
TC	Update Results											
TD	Response time for previous transaction											
TE	Number of time-outs											
TF	Number of card reader errors											
TG	Number of unsupported cards											
TH	Number of communication errors between CAD and Merchant Application											
TI	Number of System Faults			O							O	
TJ	Number of Fatal Errors			O							O	
TK	Application Status Words											
TP	PSAM version			M							M	
TQ	PSAM Life Cycle State			O							O	
TR	PSAM Date			O							O	
TS	Grand Total											

2-14 Commands and Responses

2-14.1 Introduction

This section defines the formats for commands and responses in the terminal.

The detailed definitions of the data elements are given in section 2-15 page 2-15-1: "Data Elements".

2-14.2 Command Overview

Table 2-14.1 - Command Overview

Application	Command	MT	CLA	INS	Comments
General	Read Magnetic Stripe	'40'	–	–	Defined in ref. 27
	ICC Command	'42'	–	–	Defined in ref. 27
	ICC Command	'48'	–	–	Defined in ref. 27
	ICC Power-On	'43'	–	–	Defined in ref. 27
	ICC Power-Off	'44'	–	–	Defined in ref. 27
	ICC Query	'45'	–	–	Defined in ref. 27
	Verify Offline PIN	'46'	–	–	Defined in ref. 27
	Verify Offline PIN	'47'	–	–	Defined in ref. 27
	Confirm Amount	'60'	–	–	Defined in ref. 27
	Display Message	'61'	–	–	Defined in ref. 27
	Print Message	'63'	–	–	Defined in ref. 27
	Purge Print Buffer	'64'	–	–	Defined in ref. 27
	Get Key Check Value	'65'	–	–	Defined in ref. 27
	Get Key Check Value 2	'65'	–	–	Defined in section 2–14.5.11, page 2–14–46
	Verify PSAM Public Key Certificate	'66'	–	–	Defined in ref. 27
	Get PIN Pad Public Key Record	'67'	–	–	Defined in ref. 27
	Submit Initial Key	'68'	–	–	Defined in ref. 27
	Submit Initial Key 2	'68'	–	–	Defined in section 2–14.5.4, page 2–14–24
	Initiate PIN Entry	'69'	–	–	Defined in ref. 27
	Initiate PIN Entry 2	'69'	–	–	Defined in section 2–14.6.28, page 2–14–112
	Get PIN	'6A'	–	–	Defined in ref. 27
	Terminate PIN Entry	'6C'	–	–	Defined in ref. 27.
	Get Amount 3	'80'	–	–	Defined in section 2–14.6.29, page 2–14–114
Transaction Completed	'81'	–	–	Defined in ref. 27.	
Create File	'90'	–	–	Defined in ref. 27.	

Table 2-14.1 - Command overview (*continued*)

Application	Command	MT	CLA	INS	Comments
	Delete File	'91'	–	–	Defined in ref. 27.
	Add File Record	'92'	–	–	Defined in ref. 27.
	Get File Record	'93'	–	–	Defined in ref. 27.
	Update File Record	'94'	–	–	Defined in ref. 27.
	Find and Get File Record	'95'	–	–	Defined in ref. 27.
	Delete File Record	'96'	–	–	Defined in ref. 27.
	Find and Delete File Record	'97'	–	–	Defined in ref. 27.
	Clear File	'98'	–	–	Defined in ref. 27.
	Initiate Communication Session	'B0'	–	–	Defined in ref. 27.
	Terminate Communication Session	'B1'	–	–	Defined in ref. 27.
	Add Event to Queue	'C0'	–	–	Defined in ref. 27.
	Get Event from Queue	'C1'	–	–	Defined in ref. 27.
	Find event on Queue	'C2'	–	–	Defined in ref. 27.
	Flush Event Queue	'C3'	–	–	Defined in ref. 27.
	Open Handler	'F0'	–	–	Defined in ref. 27.
	Close Handler	'F1'	–	–	Defined in ref. 27.
	Write Handler String	'F3'	–	–	Defined in ref. 27.
	Read Handler String	'F4'	–	–	Defined in ref. 27.
	Get Handler Address	'F5'	–	–	Defined in ref. 27.
Application Selection	Select	'42'	'00'	'A4'	Defined in ref. 20.
	Read Record	'42'	'00'	'B2'	Defined in ref. 20.
Proprietary	Check Stop List	'01'	–	–	Defined in section 2-14.6.19, page 2-14-97
	Verify Signature	'02'	–	–	Defined in section 2-14.6.20, page 2-14-99
	Load LP Keys	'42'	'B1'	'00'	Defined in section 2-14.8.1, page 2-14-122
	Verify Local PIN	'42'	'B1'	'80'	Defined in section 2-14.8.2, page 2-14-124
	Get Merchant Data	'04'	–	–	Defined in section 2-14.6.21, page 2-14-100
	Transaction State Information	'05'	–	–	Defined in section 2-14.6.22, page 2-14-102
	Repeat Last ICC Response	'06'	–	–	Defined in section 2-14.6.23, page 2-14-104
	Submit Card Reference	'07'	–	–	Defined in section 2-14.6.24, page 2-14-105
	Submit Card Reference2	'08'	–	–	Defined in section 2-14.6.25, page 2-14-107
	Retrieve Card Data MSC	'42'	'B0'	'7E'	Defined in section 2-14.6.26, page 2-14-109
	Retrieve Card Data ICC	'42'	'B0'	'7E'	Defined in section 2-14.6.27, page 2-14-111

Table 2-14.1 - Command overview (*continued*)

Application	Command	MT	CLA	INS	Comments
Application Specific (Debit/Credit)					
Administrative	Install	'42'	'B0'	'70'	Defined in section 2–14.5.1, page 2–14–20
	Install 2	'42'	'B0'	'70'	Defined in section 2–14.5.2, page 2–14–21
	Validate Install Data	'42'	'B0'	'7A'	Defined in section 2–14.5.3, page 2–14–23
	Add Addendum Record	'42'	'B0'	'72'	Defined in section 2–14.5.5, page 2–14–26
	Deactivate PSAM	'42'	'B0'	'74'	Defined in section 2–14.5.6, page 2–14–27
	Create Service Record	'42'	'B0'	'76'	Defined in section 2–14.5.7, page 2–14–28
	Get Debit/Credit Properties	'42'	'B0'	'A0'	Defined in section 2–14.5.8, page 2–14–29
	Set Debit/Credit Properties	'42'	'B0'	'A0'	Defined in section 2–14.5.9, page 2–14–41
	Get Random Number	'42'	'B0'	'A0'	Defined in section 2–14.5.10, page 2–14–44
	Get Processing Condition Table	'42'	'B0'	'3A'	Defined in section 2–14.5.12, page 2–14–47
	PSAM Update	'42'	'B4'	'48'..'4E'	Defined in section 2–14.5.13, page 2–14–52
EMV	Initiate EMV Payment 2	'42'	'B0'	'80'	Defined in section 2–14.6.1, page 2–14–54
	EMV Payment	'42'	'B0'	'82'	Defined in section 2–14.6.2, page 2–14–57
	Validate Data 2	'42'	'B0'	'84'	Defined in section 2–14.6.3, page 2–14–59
	Complete Payment	'42'	'B0'	'8E'	Defined in section 2–14.6.4, page 2–14–65
MSC	Initiate MSC Payment 2	'42'	'B0'	'80'	Defined in section 2–14.6.5, page 2–14–66
	MSC Payment	'42'	'B0'	'82'	Defined in section 2–14.6.7, page 2–14–71
	Validate Data 2	'42'	'B0'	'84'	Defined in section 2–14.6.3, page 2–14–59
	Complete Payment	'42'	'B0'	'8E'	Defined in section 2–14.6.8, page 2–14–73
Key Entered	Initiate Key Entered Payment	'42'	'B0'	'80'	Defined in section 2–14.6.9, page 2–14–74
	Key Entered Payment	'42'	'B0'	'82'	Defined in section 2–14.6.11, page 2–14–79
	Validate Data 2	'42'	'B0'	'84'	Defined in section 2–14.6.3, page 2–14–59
	Complete Payment	'42'	'B0'	'8E'	Defined in section 2–14.6.12, page 2–14–81

Table 2-14.1 - Command overview (*concluded*)

Application	Command	MT	CLA	INS	Comments
Token based	Initiate Token Based Payment 2	'42'	'B0'	'80'	Defined in section 2-14.6.13, page 2-14-82
	Token Based Payment	'42'	'B0'	'82'	Defined in section 2-14.6.14, page 2-14-85
	Validate Data 2	'42'	'B0'	'84'	Defined in section 2-14.6.3, page 2-14-59
	Complete Payment	'42'	'B0'	'8E'	Defined in section 2-14.6.15, page 2-14-87
Contactless	Initiate Contactless Payment	'42'	'B0'	'80'	Defined in section < - >, page < - - >
	Contactless Payment	'42'	'B0'	'82'	Defined in section < - >, page < - - >
	Validate Data 2	'42'	'B0'	'84'	Defined in section < - >, page < - - >
	Complete Payment	'42'	'B0'	'8E'	Defined in section < - >, page < - - >
Cancellation	Initiate Cancellation Payment	'42'	'B0'	'80'	Defined in section 2-14.7.1, page 2-14-117
	Cancellation Payment	'42'	'B0'	'82'	Defined in section 2-14.7.2, page 2-14-119
	Validate Data 2	'42'	'B0'	'84'	Defined in section 2-14.6.3, page 2-14-59
	Complete Payment	'42'	'B0'	'8E'	Defined in section 2-14.7.3, page 2-14-120
PSAM Initialization (Generic)					
	Start-up PSAM	'42'	'B0'	'02'	Defined in section 2-14.4.1, page 2-14-8
	PSAM Shutdown	'42'	'B0'	'04'	Defined in ref. 27
	Get Supported AIDs	'42'	'B0'	'08'	Defined in section 2-14.4.2, page 2-14-9
	Synchronize PSAM/PIN Pad	'42'	'B0'	'C2'	Defined in section 2-14.4.6, page 2-14-16
	Get Next	'42'	'B0'	'FC'	Defined in ref. 27
	Response Command	'42'	'B0'	'FE'	Defined in ref. 27
Application Specific PSAM Initialization (Debit/Credit)					
	Get MSC Table	'42'	'B0'	'30'	Defined in section 2-14.4.3, page 2-14-11
	Get Debit/Credit File Characteristics	'42'	'B0'	'32'	Defined in section 2-14.4.4, page 2-14-13
	Exchange Debit/Credit Static Information	'42'	'B0'	'3C'	Defined in section 2-14.4.8, page 2-14-18
	Configure PSAM Application	'42'	'B0'	'3E'	Defined in section 2-14.4.5, page 2-14-15

For PSAM commands and responses, the portion which is part of the command APDU or the response generated by the PSAM is shaded.

TAPA defined commands are listed in this specification only when additional proprietary Application Status Words are defined.

Table 2-14.2 - Command - Handler Overview

Command	MT	CLA	INS	Destination Address	Source Address
Check Stop List	'01'			'0400' (Merchant Application)	'00pp' (PSAM)
Verify Signature	'02'			'0400' (Merchant Application)	'0100' (MAD-Handler)
Verify LP Keys	'42'	'B1'	'00'	'0301' (PIN Pad)	'00pp' (PSAM)
Verify Local PIN	'42'	'B1'	'80'	'0301' (PIN Pad)	'00pp' (PSAM)
Get Merchant Data	'04'			'0400' (Merchant Application)	'00pp' (PSAM)
Transaction State Information	'05'			'0400' (Merchant Application)	'00pp' (PSAM)
Repeat Last ICC Response	'06'			'0202' (Processor Card Handler)	'00pp' (PSAM)
Submit Card Reference	'07'			'0400' (Merchant Application)	'00pp' (PSAM)
Read Magnetic Stripe	'40'			'0201' (Magnetic stripe reader)	Any
ICC Command	'42'			'0202' (Processor card reader) '00pp' (PSAM)	Any
Select	'42'	'00'	'A4'	'0202' (Processor Card Handler)	'0100' (MAD-Handler)
Start-up PSAM	'42'	'B0'	'02'	'00pp' (PSAM)	'0100' (MAD-Handler)
PSAM Shutdown	'42'	'B0'	'04'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get Supported AIDs	'42'	'B0'	'08'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get MSC Table	'42'	'B0'	'30'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get Debit/Credit File Characteristics	'42'	'B0'	'32'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get Processing Condition Table	'42'	'B0'	'3A'	'00pp' (PSAM)	'0100' (MAD-Handler)
Exchange Debit/Credit Static Information	'42'	'B0'	'3C'	'00pp' (PSAM)	'0100' (MAD-Handler)
Configure PSAM Application	'42'	'B0'	'3E'	'00pp' (PSAM)	'0100' (MAD-Handler)
Install	'42'	'B0'	'70'	'00pp' (PSAM)	'0100' (MAD-Handler)
Install 2	'42'	'B0'	'70'	'00pp' (PSAM)	'0100' (MAD-Handler)
Add Addendum Record	'42'	'B0'	'72'	'00pp' (PSAM)	'0100' (MAD-Handler)
Deactivate PSAM	'42'	'B0'	'74'	'00pp' (PSAM)	'0100' (MAD-Handler)
Create Service Record	'42'	'B0'	'76'	'00pp' (PSAM)	'0100' (MAD-Handler)
Validate Install Data	'42'	'B0'	'7A'	'00pp' (PSAM)	'0100' (MAD-Handler)
Initiate Payment	'42'	'B0'	'80'	'00pp' (PSAM)	'0100' (MAD-Handler)
Payment	'42'	'B0'	'82'	'00pp' (PSAM)	'0100' (MAD-Handler)
Validate Data	'42'	'B0'	'84'	'00pp' (PSAM)	'0100' (MAD-Handler)
Complete Payment	'42'	'B0'	'8E'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get Debit/Credit Properties	'42'	'B0'	'A0'	'00pp' (PSAM)	'0100' (MAD-Handler)
Synchronize PSAM/PIN Pad	'42'	'B0'	'C2'	'00pp' (PSAM)	'0100' (MAD-Handler)
Set Debit/Credit Properties	'42'	'B0'	'A0'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get Processing Condition Table	'42'	'B0'	'3A'	'00pp' (PSAM)	'0100' (MAD-Handler)
Get Next	'42'	'B0'	'FC'	'00pp' (PSAM)	
Response Command	'42'	'B0'	'FE'	'00pp' (PSAM) '0202' (Processor Card Handler)	Any
Load Card Data Protection Keys	'42'	'B2'	'00'	'00pp' (PSAM)	'0100' (MAD-Handler)
Legend: Grey area indicates TAPA defined commands.					

Table 2-14.2 - Command - Handler Overview (*continued*)

Command	MT	CLA	INS	Destination Address	Source Address
PSAM Update	'42'	'B4'	'48/ '4E'	'00pp' (PSAM)	'0100' (MAD-Handler)
ICC Command	'42'			'0202' (Processor card reader)	Any
Verify	'42'	'00'	'20'	'0202' (Processor card reader)	'00pp' (PSAM)
External Authenticate	'42'	'00'	'82'	'0202' (Processor card reader)	'00pp' (PSAM)
Get Challenge	'42'	'00'	'84'	'0202' (Processor card reader)	'00pp' (PSAM)
Internal Authenticate	'42'	'00'	'88'	'0202' (Processor card reader)	'00pp' (PSAM)
Read Record	'42'	'00'	'B2'	'0202' (Processor card reader)/ '0204' (Contactless card reader)	'00pp' (PSAM)
Put Data	'42'	'04'	'DA'	'0204' (Contactless card reader)	'00pp' (PSAM)
Get Processing Options	'42'	'80'	'A8'	'0202' (Processor card reader)/ '0204' (Contactless card reader)	'00pp' (PSAM)
Generate AC	'42'	'80'	'AE'	'0202' (Processor card reader)	'00pp' (PSAM)
Get Data	'42'	'80'	'CA'	'0202' (Processor card reader)/ '0204' (Contactless card reader)	'00pp' (PSAM)
Card Block	'42'	'84'/'8C'	'16'	'0202' (Processor card reader)	'00pp' (PSAM)
Application Unblock	'42'	'84'/'8C'	'18'	'0202' (Processor card reader)	'00pp' (PSAM)
Application Block	'42'	'84'/'8C'	'1E'	'0202' (Processor card reader)	'00pp' (PSAM)
PIN Change/Unblock	'42'	'84'/'8C'	'24'	'0202' (Processor card reader)	'00pp' (PSAM)
ICC Power-On	'43'			'0202' (Processor card reader)	Any
ICC Power-Off	'44'			'0202' (Processor card reader)	Any
ICC Query	'45'			'0202' (Processor card reader)	Any
Verify Offline PIN	'46'			'0202' (Processor card reader)	Any
Confirm Amount	'60'			'0300' (User Interface Handler)	Any
Display Message	'61'			'0304' (Customer display) '0404' (Merchant display)	Any
Print Message	'63'			'0302' (Customer printer) '0402' (Merchant printer)	Any
Purge Print Buffer	'64'			'0302' (Customer printer)	Any
Get Key Check Value	'65'			'0301' (PIN Pad)	Any
Get Key Check Value 2	'65'			'0301' (PIN Pad)	Any
Verify PSAM Public Key Certificate	'66'			'0301' (PIN Pad)	Any
Get PIN Pad Public Key Record	'67'			'0301' (PIN Pad)	Any
Submit Initial Key	'68'			'0301' (PIN Pad)	Any
Submit Initial Key 2	'68'			'0301' (PIN Pad)	Any
Initiate PIN Entry	'69'			'0301' (PIN Pad)	Any
Initiate PIN Entry 2	'69'			'0301' (PIN Pad)	Any
Get PIN	'6A'			'0301' (PIN Pad)	Any
Terminate PIN Entry	'6C'			'0301' (PIN Pad)	Any
Get Amount 3	'80'			'0300' (User Interface Handler) '0400' (Merchant Application Handler)	Any
Legend: Grey area indicates TAPA defined commands.					

Table 2-14.2 - Command - Handler Overview (*concluded*)

Command	MT	CLA	INS	Destination Address	Source Address
Transaction Completed	'81'			'0400' (Merchant Application)	Any
Create File	'90'			'0500' (Data Store Handler)	Any
Delete File	'91'			'0500' (Data Store Handler)	Any
Add File Record	'92'			'0500' (Data Store Handler)	Any
Get File Record	'93'			'0500' (Data Store Handler)	Any
Update File Record	'94'			'0500' (Data Store Handler)	Any
Find and Get File Record	'95'			'0500' (Data Store Handler)	Any
Delete File Record	'96'			'0500' (Data Store Handler)	Any
Find and Delete File Record	'97'			'0500' (Data Store Handler)	Any
Clear File	'98'			'0500' (Data Store Handler)	Any
Initiate Communication Session	'B0'			'0600' (Communication Handler)	Any
Terminate Communication Session	'B1'			'0600' (Communication Handler)	Any
Add Event to Queue	'C0'			'0700' (Event Handler)	Any
Get Event from Queue	'C1'			'0700' (Event Handler)	Any
Find event on Queue	'C2'			'0700' (Event Handler)	Any
Flush Event Queue	'C3'			'0700' (Event Handler)	Any
Open Handler	'F0'			Any	Any
Close Handler	'F1'			Any	Any
Write Handler String	'F3'			Any	Any
Read Handler String	'F4'			Any	Any
Get Handler Address	'F5'			XX00 (Handler category)	Any
Legend:					
Grey area indicates TAPA defined commands.					

2-14.3 Error Responses

2-14.3.1 MAD-Handler Interface to the PSAM

- 2-14.3.1.1 A The format of error responses will be according to ref. 27: "TAPA, Application Architecture Specification" and ref. 28: "TAPA, Application Architecture Specification - Errata".

2-14.4 Commands used during Initialization

The following sections, 2-14.4.1 to 2-14.4.8, detail the commands and responses between the MAD-Handler and the PSAM used during initialization/power-up.

2-14.4.1 Start-up PSAM

Command Message

- 2-14.4.1.1 A The *Start-up PSAM* command shall conform to the format defined in table 2-14.3.

Table 2-14.3 - Command message for the *Start-up PSAM* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'02'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier	1
PSAM sub-address	'pp' – sub-address at which the PSAM is located	1
L _e	'00'	1

Response Message

A *successful* response to the *Start-up PSAM* command has the format defined in table 2-14.4.

- 2-14.4.1.2 A A Response shall be considered successful when the Application Status Words (ASW1-ASW2) have one of the following values: '0000', '1000', '1001', '1002' and '1003'.

Table 2-14.4 - Successful response message for the *Start-up PSAM* command

Field	Value	Length (bytes)
Destination Address	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0011'	2
PSAM Identification	RID _{PSAM} ID _{PSAMCREATOR} ID _{PSAM}	13
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

2-14.4.2 Get Supported AIDs

Command Message

- 2-14.4.2.1 A The *Get Supported AIDs* command shall conform to the format defined in table 2-14.5.

Table 2-14.5 - Command message for the *Get Supported AIDs* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0007'	2
CLA	'B0'	1
INS	'08'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'01'	1
ID _{THREAD}	Thread Identifier	1
L _e	'00'	1

Response Message

A successful response to the *Get Supported AIDs* command has the format defined in table 2-14.6.

Table 2-14.6 - Successful response message for the *Get Supported AIDs* command

Field	Value	Length (bytes)
Destination Address	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CNT _{AID}	Number of AIDs listed in this response The following fields (sub-scripted by "N") are repeated CNT _{AID} times (N = 1 to CNT _{AID})	1
LEN _{AIDN}	Length of Nth AID	1
AID _N	Nth AID	5 – 16
ID _{SCHEME, N}	A reference number assigned to AID N by the acquirer	1
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.4.3 Get MSC Table

Command Message

- 2-14.4.3.1 A The *Get MSC Table* command shall conform to the format defined in table 2-14.7.

Table 2-14.7 - Command message for the *Get MSC Table* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'30'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier	1
Start Location	'00' = Start at first MSC Table entry, get full table '01' = Start at next MSC Table entry, get full table '02' = Start at first MSC Table entry, Private label only '03' = Start at next MSC Table entry, Private label only	1
L _e	'00'	1

Response Message

A *successful* response to the *Get MSC Table* command has the format defined in table 2-14.8.

Table 2-14.8 - Successful response message for the *Get MSC Table* command

Field	Value	Length (bytes)
Destination Address	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CNT _{MSC}	Number of MSC records in this response. The following fields (indicated as MSC record) are repeated CNT _{MSC} times.	2
MSC record		
PAN _{FROM}	PAN range from	4 or 6 ¹⁾
PAN _{TO}	PAN range to	4 or 6 ¹⁾
Continuation Indicator	'00' = Information for every supported MSC Table has been retrieved. 'FF' = More MSC Table entries available. Re-issue command to retrieve	1
ASW1-ASW2	Application Status Words	2
RC	'0000'	2
Legend:		
1) The length of the response depends on the value of the Start Location.		
0 or 1: 4 bytes will be returned		
2 or 3: 6 bytes will be returned.		

2-14.4.4 Get Debit/Credit File Characteristics

Command Message

- 2-14.4.4.1 A The *Get Debit/Credit File Characteristics* command shall conform to the format defined in table 2-14.9.

Table 2-14.9 - Command message for the *Get Debit/Credit File Characteristics* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0007'	2
CLA	'B0'	1
INS	'32'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'01'	1
ID _{THREAD}	Thread Identifier	1
L _e	'00'	1

Response Message

A successful response to the *Get Debit/Credit File Characteristics* command has the format defined in table 2-14.10.

Table 2-14.10 - Successful response message for the *Get Debit/Credit File Characteristics* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0018'	2
Administrative File		
NUM _{FILE}	Number of files. '00' or '01' depending on whether or not the PSAM uses an Administrative File	1
LEN _{KEY}	Length of search key ('00' if no search key is used)	1
LEN _{REC}	Maximum record length (in bytes) required	2
Priority1 Files		
NUM _{FILE}	'01' ('00' if priority1 File is not used)	1
LEN _{KEY}	Length of search key ('00' if no search key is used)	1
LEN _{REC}	Maximum record length (in bytes) required	2
Priority2 Files		
NUM _{FILE}	'01' ('00' if priority2 File is not used)	1
LEN _{KEY}	Length of search key ('00' if no search key is used)	1
LEN _{REC}	Maximum record length (in bytes) required	2
Priority3 Files		
NUM _{FILE}	'01' ('00' if priority3 File is not used)	1
LEN _{KEY}	Length of search key ('00' if no search key is used)	1
LEN _{REC}	Maximum record length (in bytes) required	2
Priority4 Files		
NUM _{FILE}	'01' ('00' if priority4 File is not used)	1
LEN _{KEY}	Length of search key ('00' if no search key is used)	1
LEN _{REC}	Maximum record length (in bytes) required	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.4.5 Configure PSAM Application

Command Message

- 2-14.4.5.1 A The *Configure PSAM Application* command shall conform to the format defined in table 2-14.11.

Table 2-14.11 - Command message for the *Configure PSAM Application* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'3E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier	1
FILEID _{ADMIN}	File identifier for the administrative file Shall be zeroes if the administrative file is not used.	2
FILEID _{PRIORITY,n}	A list of file identifiers for the priority files	2*n
L _e	'00'	1

Response Message

A *successful* response to the *Configure PSAM Application* command has the format defined in table 2-14.12.

Table 2-14.12 - Successful response message for the *Configure PSAM Application* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0004'	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.4.6 Synchronize PSAM/PIN Pad

Command Message

- 2-14.4.6.1 A The *Synchronize PSAM/PIN Pad* command shall conform to the format defined in table 2-14.13.

Table 2-14.13 - Command message for the *Synchronize PSAM/PIN Pad* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0007'	2
CLA	'B0'	1
INS	'C2'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'01'	1
ID _{THREAD}	Thread Identifier	1
L _e	'00'	1

Response Message

A *successful* response to the *Synchronize PSAM/PIN Pad* command has the format defined in table 2-14.14.

Table 2-14.14 - Successful response message for the *Synchronize PSAM/PIN Pad* command

Field	Value	Length (bytes)
Destination Address	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000C'	2
PIN Pad Identifier		
ID _{PPCREATOR}	Unique ID of PIN Pad Creator	4
ID _{PP}	Unique ID of PIN Pad	4
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.4.7 Get Next

Command Message

- 2-14.4.7.1 A The *Get Next* command shall conform to the format defined in table 2-14.15.

Table 2-14.15 - Command message for the *Get Next* command

Field	Value	Length (bytes)
CLA	'B0'	1
INS	'FC'	1
P1	ID _{THREAD}	1
P2	'00'	1
L _e	'00'	1

Response Message

A *successful* response to the *Get Next* command has the format defined in table 2-14.16.

Table 2-14.16 - Successful response message for the *Get Next* command

Field	Value	Length (bytes)
Response Data	Next increment of Response Data	Variable
SW1 SW2	Status Words	2

Status Words

The Status Words (SW1 SW2) applicable for the *Get Next* command are defined in table 2-14.17.

Table 2-14.17 - Status Words applicable for the *Get Next* command

SW1 SW2	Meaning	Usage
'9000'	Successful	Last increment of data to be given to the PSAM
'9601'	Get next incremental response	The PSAM Handler must issue a new Get Next command to get the remaining Response Data

2-14.4.8 Exchange Debit/Credit Static Information

Command Message

- 2-14.4.8.1 A The *Exchange Debit/Credit Static Information* command shall have the format shown in table 2-14.18.

Table 2-14.18 - Command message of the *Exchange Debit/Credit Static Information* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0025'	2
CLA	'B0'	1
INS	'3C'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'1F'	1
ID _{THREAD}	Thread Identifier	1
Terminal Capabilities	Terminal Capabilities according to ref. 20: "EMV ICC Specification"	3
Additional Terminal Capabilities	Additional Terminal Capabilities according to ref. 20: "EMV ICC Specification"	5
Software Version Number	Software Version Number	2
Hardware Version Number	Hardware Version Number	2
Terminal Approval No.	Unique number identifying a certified Terminal	2
MAD-Handler ID	Unique identifier of the terminal equipment	8
Terminal Type	Terminal Type according to ref. 20: "EMV ICC Specification"	1
POS Capability Code	Point of Sale Capability Code. See section 2-13.9.4.	6
Info Level	Merchant Application Log requested or not & PSAM State Information send to Merchant Application or not.	1
L _e	'00'	1

Response Message

A successful response to the *Exchange Debit/Credit Static Information* command has the format shown in table 2-14.19.

- 2-14.4.8.2 A A Response shall be considered successful when the Application Status Words (ASW1-ASW2) have one of the following values: '0000', '1001', '1002' and '1003'.

Table 2-14.19 - Successful response message for the *Exchange Debit/Credit Static Information* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0071'	2
Signature Verification	'00' = Signature verification by merchant is not required 'FF' = Signature verification by merchant is required	1
CNT _{ENTRIES}	The number of transaction entries available to the PSAM Debit/Credit application. This is the number of simultaneous open transactions that the PSAM can accommodate.	1
ME _{NUMBER}	Merchant No. assigned by Nets Denmark A/S	5
ME _{NAME}	Merchant Name	18
ME _{CITY}	Merchant City Name	16
ME _{ADDRESS}	Merchant Address	24
ME _{ZIP}	Merchant Postal Code	8
ME _{PHONE}	Merchant Phone No.	24
ME _{BRN}	Merchant Business Registration Number (CVR-Number)	12
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.5 Debit/Credit Administrative Commands

2-14.5.1 Install

Command Message

- 2-14.5.1.1 A The *Install* command shall have the format shown in table 2-14.20.

Table 2-14.20 - Command message of the *Install* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0025'	2
CLA	'B0'	1
INS	'70'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'1F'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Terminal Capabilities	Terminal Capabilities according to ref. 20: "EMV ICC Specification"	3
Additional Terminal Capabilities	Additional Terminal Capabilities according to ref. 20: "EMV ICC Specification"	5
Software Version Number	Software Version Number	2
Hardware Version Number	Hardware Version Number	2
Terminal Approval No.	Unique number identifying a certified Terminal	2
MAD-Handler ID	Unique identifier of the terminal equipment	8
Terminal Type	Terminal Type according to ref. 20: "EMV ICC Specification"	1
POS Capability Code	Point of Sale Capability Code. See section 2-13.9.4.	6
Info Level	Merchant Application Log requested or not & PSAM State Information send to Merchant Application or not.	1
L _e	'00'	1

Response Message

A *successful* response to the *Install* command has the format shown in table 2-14.21.

Table 2-14.21 - Successful response message for the *Install* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{HREQ}	Length of host request (Install)	2
Host Request	Host request message	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.5.2 Install 2

Command Message

- 2-14.5.2.1 A The *Install 2* command shall have the format shown in table 2-14.22.

Table 2-14.22 - Command message of the *Install 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0025'	2
CLA	'B0'	1
INS	'70'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'35' + LEN _{PCIDATA}	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1

Table 2-14.22 - Command message of the *Install 2* command (*concluded*)

Terminal Capabilities	Terminal Capabilities according to ref. 20: "EMV ICC Specification"	3
Additional Terminal Capabilities	Additional Terminal Capabilities according to ref. 20: "EMV ICC Specification"	5
Software Version Number	Software Version Number	2
Hardware Version Number	Hardware Version Number	2
Terminal Approval No.	Unique number identifying a certified Terminal	2
MAD-Handler ID	Unique identifier of the terminal equipment	8
Terminal Type	Terminal Type according to ref. 20: "EMV ICC Specification"	1
POS Capability Code	Point of Sale Capability Code. See section 2-13.9.4.	6
Info Level	Merchant Application Log requested or not & PSAM State Information send to Merchant Application or not.	1
PED Data		
ALG _{PPSYNC}	Information on supported algorithm and key length	1
ID _{PPCREATOR}	Identifier of the PED Creator	4
ID _{PP}	Identifier assigned to the PIN Pad by the PIN Pad Creator	4
PED BDK Version No.	Data used by the host to select the PED Base Derivation Key	4
PED KEK Deriv. Data	Data used to compute the new PED Key Encryption Key (PED KEK Version Number PED KEK Date)	8
LEN _{PCIData}	No. of bytes in PCI Data	1
PCI Data	TLV coded information on terminal parameters	Var.
L _e	'00'	1

NOTE: The PSAM will distinguish between the *Install* and the *Install 2* command based on the overall length of the command.

NOTE: The field PCI Data consist of a number TLV coded terminal parameters. See section 2-15.2.102 (Data Elements) for further details.

Response Message

A *successful* response to the *Install 2* command has the format shown in table 2-14.23. This is identical to the format of the *Install* response except for the larger size of the Host Request due to extra data elements.

Table 2-14.23 - Successful response message for the *Install 2* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{HREQ}	Length of host request (Install)	2
Host Request	Host request message	Var.
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.5.3 Validate Install Data

Command Message

- 2-14.5.3.1 A The *Validate Install Data* command shall have the format shown in table 2-14.24.

Table 2-14.24 - Command message of the *Validate Install Data* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'7A'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
LEN _{HR}	Length of host data (if no online connection then equal to '00')	2
Host Response	Host response data	Variable
L _e	'00'	1

Response Message

A successful response to the *Validate Install Data* command has the format shown in table 2-14.25.

Table 2-14.25 - Successful response message for the *Validate Install Data* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0004'	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.5.4 Submit Initial Key 2

Command Message

The *Submit Initial Key 2* command has the format shown in table 2-14.26.

Table 2-14.26 - Command message of the *Submit Initial Key 2* command

Field	Value	Length (bytes)
Destination Address	'0301' for the User Interface, PIN Pad	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'68'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0025'	2
PSAM Identification		
RID _{PSAM}	RID used by the PSAM Creator	5
ID _{PSAMCREATOR}	Identifier assigned to the PSAM Creator by the owner of the RID	4
ID _{PSAM}	Identifier assigned by the PSAM Creator to the PSAM	4
[PED Session Derivation Key] _{PEDKEK}	PED Session Derivation Key enciphered by the PED Key Encryption Key	16
PED KEK Derivation Data	Data needed to derive the new PED Key Encryption Key from the PED Master Key	8
KCV _{SDK}	KCV for the System Derivation Key	3

2-14.5.4.1 A The PED shall initially derive and temporarily save the PED Key Encryption Key. It shall then decrypt the SDK using the PED KEK, calculate the KCV_{SDK} and compare the value to the KCV received in the command.

2-14.5.4.2 A The PED shall return a response code of 'FF8A' if the received and the computed KCV does not match

Response Message

2-14.5.4.3 A A *successful* response to the *Submit Initial Key 2* command shall have the format shown in table 2-14.27.

2-14.5.4.4 A An *unsuccessful* response to the *Submit Initial Key 2* command shall return a response code of 'FF8A'

Table 2-14.27 - Successful response message for the *Submit Initial Key 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0301'	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0002'	2
RC	'0000'	2

NOTE: There are no return parameters to the *Submit Initial Key 2* command.

2-14.5.5 Add Addendum Record

Command Message

- 2-14.5.5.1 A The *Add Addendum Record* command shall have the format shown in table 2-14.28.

Table 2-14.28 - Command message of the *Add Addendum Record* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'72'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Addendum Status	MSB: Segment number of this Addendum Record LSB: Total number of segments	2
LEN _{PAN}	Length of the Primary Account Number	1
PAN	The Primary Account Number	Up to 10
Original Data Elements		
STAN	Systems Trace Audit Number	3
Time	Time, local transaction	3
Date	Date, local transaction	2
MRC	Message Reason Code (see section 2-13.9.7)	2
Batch Number	Batch Number used for reconciliation	12
Terminal ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
MAD-Handler ID	Unique identifier of the terminal equipment	8
Terminal Approval No.	Unique number identifying a certified terminal	2
LEN _{ADD}	Length of the addendum record	2
Addendum Record	Addendum record to be linked to a previous financial transaction	Variable
L _e	'00'	1

Response Message

A *successful* response to the *Add Addendum Record* command has the format shown in table 2-14.29.

Table 2-14.29 - Successful response message for the *Add Addendum Record* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0004'	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.5.6 Deactivate PSAM

Command Message

- 2-14.5.6.1 A The *Deactivate PSAM* command shall have the format shown in table 2-14.30.

Table 2-14.30 - Command message of the *Deactivate PSAM* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0011'	2
CLA	'B0'	1
INS	'74'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'0B'	1
ID _{THREAD}	'00'	1
Terminal Approval No.	Unique number identifying a certified Terminal	2
MAD-Handler ID	Unique number identifying a certified terminal	8
L _e	'00'	1

Response Message

A successful response to the *Deactivate PSAM* command has the format shown in table 2-14.31.

Table 2-14.31 - Successful response message for the *Deactivate PSAM* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{HREQ}	Length of host request (Deactivate)	2
Host Request	Host request message	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.5.7 Create Service Record

Command Message

- 2-14.5.7.1 A The *Create Service Record* command shall have the format shown in table 2-14.32.

Table 2-14.32 - Command message of the *Create Service Record* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0007'	2
CLA	'B0'	1
INS	'76'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'01'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _e	'00'	1

Response Message

A *successful* response to the *Create Service Record* command has the format shown in table 2-14.33.

Table 2-14.33 - Successful response message for the *Create Service Record* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD–Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub–address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0004'	2
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

2-14.5.8 Get Debit/Credit Properties

Command Message

- 2-14.5.8.1 A The *Get Debit/Credit Properties* command shall have the format shown in table 2-14.34.

Table 2-14.34 - Command message of the *Get Debit/Credit Properties* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub–address assigned to the PSAM	2
Source Address	'0100' for the MAD–Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD–Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'A0'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD–Handler	1
Identifier	Identifies the Property / data element to be requested (see table 2–14.36)	2
LEN _{INFO}	Length of the Additional Info ('00' if absent)	1
Additional Info	Present if additional information is required (see table 2–14.36)	Variable
L _e	'00'	1

Response Message

A *successful* response to the *Get Debit/Credit Properties* command has the format shown in table 2-14.35.

Table 2-14.35 - Successful response message for the *Get Debit/Credit Properties* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{PROPERTY}	Length of the properties requested ('0000' if absent)	2
Property	Property / Data element (see table 2-14.36)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

Table 2-14.36 - Properties / Data Elements to be Requested

Identifier	Property / Data Element	Command		Response	
		Additional Info		Property	
		Data Element	Length	Data Element	Length
'0001'	Additional AID Info	AID (from AID table)	5 – 16	Card Name	16
				ASI	1
'0002'	Additional MSC Info	LEN _{TRACK2/TRACK3}	1	Card Name	16
		Track2 Data or	Up to 19	Card Service Info ⁸⁾	1
		Track3 Data	52	Service Code	0 or 2 ¹⁾
'0003'	Additional PSAM Info	(Empty)	0	PSAM Identifier ²⁾	13
				PSAM Version	1
				PSAM Subversion	1
				PSAM D/C Life Cycle State	1
				Service Packs supported	1
				LEN _{DD} (Length of Discretionary Data)	1
		Discretionary Data	Var.		
'0004'	Previous Transaction Status	Reference STAN	3	Reference STAN	3
				Amount	4
				CURRC	2
				CURRE	1
				DTHR	5
'0005'	Previous Transaction Status	LEN _{PAN} ³⁾	1	Reference STAN	3
		PAN ⁴⁾	Up to 10	Amount	4
				CURRC	2
				CURRE	1
				DTHR	5

Table 2-14.36 - Properties / Data Elements to be Requested (*continued*)

Identifier	Property / Data Element	Command		Response	
		Additional Info		Property	
		Data Element	Length	Data Element	Length
'0006'	Retrieve Local PIN Information	(Empty)	0	Transaction Counter (0)	4
				LP-KEK-Version (0) ⁵⁾	1
				LP-PPK-Version (0)	1
				Transaction Counter (1)	4
				LP-KEK-Version (1)	1
				LP-PPK-Version (1)	1
				Transaction Counter (2)	4
				LP-KEK-Version (2)	1
				LP-PPK-Version (2)	1
				Transaction Counter (3)	4
				LP-KEK-Version (3)	1
		LP-PPK-Version (3)	1		
'0007'	Checksum Data	LEN _{Terminal Checksum}	1 ⁶⁾	EMV Checksum	8
		Terminal Checksum	up to 200	PSAM Code Checksum	8
				PSAM Config Checksum	8
'0008'	Issuer Envelope buffer size	(Empty)	0	Max. length (bytes) of issuer envelope data for MSC transactions	1
				Max. length (bytes) of issuer envelope data for EMV transactions	1
'0009'	Extended AID Info	AID (from AID table)	5 – 16	Response is TLV-coded. See table 2-14.37 for exact contents	Var.
'000A'	Retrieve Reference STAN	(Empty)	0	Reference STAN	3
'000B'	Retrieve TVR/ TSI/IAC	(Empty)	0	TVR (Tag '95')	5
				TSI (Tag '9B')	2
				IAC (Default, Tag '9F0D')	5
				IAC (Denial, Tag '9F0E')	5
				IAC (Online, Tag '9F0F')	5

Table 2-14.36 - Properties/Data Elements to be Requested (*continued*)

Identifier	Property / Data Element	Command		Response	
		Additional Info		Property	
		Data Element	Length	Data Element	Length
'000C'	Retrieve Contactless Amounts ⁷⁾	(Empty)	0	Initial Card Balance	4
				Final Card Balance	4
				Sign: "D"/"C" (Top Up)	1
				Top Up Amount	4
				Sign: "D"/"C" (Available Funds)	1
				Available Funds	4
				Maximum Deposit	4
'000D'	Retrieve Acquirer Information	(Empty)	0	Tag Acq ID, "BG"	2
				LEN _{AI} (Acquirer ID)	1
				Acquirer ID	..24
				Tag Acq Merch, "BH"	2
				LEN _{AM} (Acq. Mer. Num)	1
				Acquirer Merchant Num.	..24
'000E'	Retrieve Available Funds Amount	(Empty)	0	Available Funds Amount	4
'000F'	Retrieve Security Information	LEN _{SEED/TRACK} -DATA	1	Card Name	16
		Seed ⁸⁾	0 or 4	Card Service Info ¹²⁾	1
		Track Data ⁹⁾	Up to 24	Service Code ¹³⁾	2
		Mode	2	LEN _{TRACK}	1
		PIN Block Format ¹⁰⁾	0 or 1	Track Data (Clear text)	Up to 19
		Timer Flag ¹⁰⁾	0 or 1	[Online PIN]	0 or 8
		Time ¹⁰⁾	0 or 4		
		Amount ¹¹⁾	0 or 4		
		Currency Code ¹¹⁾	0 or 2		
		Currency Exponent ¹¹⁾	0 or 1		
'0010'	Get Extended Issuer Envelope Data	(Empty)	0	Extended Issuer Envelope Data	Var.

Table 2-14.36 - Properties/Data Elements to be Requested (*continued*)

Identifier	Property / Data Element	Command		Response	
		Additional Info		Property	
		Data Element	Length	Data Element	Length
'0011'	Total Issuer Envelope buffer sizes	(Empty)	0	Max. length (bytes) of Issuer Envelope Data for non-EMV transactions	2
				Max. length (bytes) of Issuer Envelope Data for EMV transactions	2
				The total length of Issuer Envelope Data and Extended Issuer Envelope Data for non-EMV transactions	2
				The total length of Issuer Envelope Data and Extended Issuer Envelope Data for EMV transactions	2
'0012'	Get MSC Tracks Information	LEN _{ALLTRACKDATA}	1	Card Name ¹⁷⁾	16
		Seed	4	Card Service Info	1
		LEN _{EncrTrack1}	1	Service Code ¹⁸⁾	2
		Encr.Track1 ¹⁴⁾	Up to 88	LEN _{Track1}	1
		LEN _{EncrTrack2}	1	Track 1 ¹⁹⁾	Up to 76
		Encr.Track2 ¹⁵⁾	Up to 24	LEN _{Track2}	1
		LEN _{EncrTrack3}	1	Track2 ¹⁹⁾	Up to 19
		Encr. Track3 ¹⁶⁾	Up to 64	LEN _{Track3}	1
				Track3 ¹⁹⁾	Up to 52
				LEN _{Trunc.PAN}	1
		Truncated PAN ²⁰⁾	Up to 10		

Table 2-14.36 - Properties/Data Elements to be Requested (*continued*)

Identifier	Property / Data Element	Command		Response	
		Additional Info		Property	
		Data Element	Length	Data Element	Length
'0013'	Get CA Public Key Information	Start Location	1	LEN _{CDP}	2
				Seed	4
				RID	5
				C _{APKI}	1
				LEN _{CAKM}	1
				C _{APKM}	Up to 248
				LEN _{CAPKE}	1
				C _{APKE}	1 or 3
		Continuation Indicator	1		
'0014'	Get Contactless AID related Information	Start Location	1	See table 2–14.38 on page 2–14–39	Up to 180
'0015'	Get Tag List for External Kernel	Kernel ID	1	LEN _{TAGLIST}	1
		Kernel Version	2	Tag List	Var.
		Technology	1		
'0016'	Retrieve PSAM Security Configuration	(Empty)	0	CNT _{LOG}	1
				Block ₁	30
				Block ₂	30
				Block _n ²¹⁾	30
'0017'	Retrieve Advice Information ²²⁾	(Empty)	0	Reference STAN	3
				Amount	4
				CURRC	2
				CURRE	1
'0018'	Get Random Number	LEN _{RandomNumber}	1	Seed	4
				[Random Number]	Var.
'0019'	Retrieve Hash Value	LEN _{Scheme Id Bitmap}	1	LEN _{Scheme Information}	2
		Scheme Id Bitmap	4	Scheme Information	n * (4+32)

Table 2-14.36 - Properties/Data Elements to be Requested (*concluded*)

'001A' – '7FFF'	Reserved for Future Use
<p>Legend:</p> <p>The coding of the data elements can be found in section 2-15, "Data Elements".</p> <ol style="list-style-type: none"> 1) Omitted if not accessible. 2) PSAM Identifier consists of RID_{PSAM} ID_{PSAMCREATOR} ID_{PSAM}. 3) Number of bytes (in case of odd number of digits, the PAN shall be padded with a trailing 'F') 4) When the PAN is used as search key, only the transaction data for the most recent successful transaction (performed with this PAN) is returned. 5) The index indicates to which key chain the information are associated. 6) Terminal Checksum shall be in the range 4 – 20 bytes. 7) If an amount is not available, the respective field will be set to all 'F's. The same goes for the sign fields. 8) Seed shall be present if the data element Mode indicates that the Track2 Data is enciphered only. 9) Clear text: The data element Track Data consist of Track2 (up to 19 bytes). Enciphered: The data element Track Data consist of Random Number (4 bytes) Track2 (up to 19 bytes) Padding according to ref. 15: "ISO/IEC 9797", Padding method 2. Track2 Data shall be enciphered if indicated in the data element Mode. 10) Fields shall be present only if the data element Mode indicates that PIN Entry are requested. 11) Fields shall be present only if the data element Mode indicates that Amount Confirmation is requested. 12) Card Service Info holds information on whether the card may be used for Private Label Card schemes or not, see section 1-10.4. 13) 'FFFF' if absent. 14) Contents of the field Encr.Track1 is: [Rnd1 (4) Track1 Data (x) '80...']KSES_{CDP}. See requirement 2-14.5.8.10. 15) Contents of the field Encr.Track2 is: [Rnd2 (4) Track2 Data (x) '80...']KSES_{CDP}. See requirement 2-14.5.8.10. 16) Contents of the field Encr.Track3 is: [Rnd3 (4) Track3 Data (x) '80...']KSES_{CDP}. See requirement 2-14.5.8.10. 17) Card name present if Track 2 is recognized by PSAM, else ASCII spaces ("2020.."). 18) If accessible / found in track2, else 'FF FF'. 19) Track data will be returned in clear text if; <ul style="list-style-type: none"> – Track2 is "non-ISO" coded, or – Track2 is "ISO" and is positively recognized as a Private Label Card, or – Track2 is not present on the card. Otherwise <u>all</u> Track data will be omitted, i.e. LEN_{Trackx} = '00'. 20) Only present if no deciphered data are returned. 21) The number of blocks returned depends on the CNT_{LOG} value. The three blocks shown are merely an example. 22) To be used in case of error handling when using Delayed Complete. 	

2-14.5.8.2

A For the Identifier '0007', the checksum values returned (PSAM Config Checksum and EMV Checksum) imply that the Initialization sequence has been completed successfully.

NOTE: The relevant data elements to be included in the PSAM Config Checksum and EMV Checksum may not

be available until the terminal is ready to perform transactions.

Table 2-14.37 - Contents of the Response when the Identifier = '0009'

Primitive Data Objects					
Tag	Attributes	Length	Applicable		Comment
			EMV	qVSDC ¹⁾	
'E4'	–	Var.	M	M	Extended AID Info Data
'DF70'	ans16	16	M	M	Card name
'DF71'	b1	1	M	M	ASI
'DF72'	b2	2	M	M	Card Product Type
'DF73'	b4	4	C	M	Card Product Functions
'DF74'	b2	2	C	M	Card Product Flow
'DF75'	–	32	C	M	Card Product EMV Entry Point Parameters
	n3	2			Currency Code
	n1	1			Currency Exponent
	b4	4			Terminal Contactless Floor Limit
	b4	4			Terminal Floor Limit
	b4	4			Terminal CVM Required Limit
	b4	4			Terminal Contactless Transaction Limit
	b1	1			Card Product Limits Flags
	b4	4			Terminal Transaction Qualifiers
	b8	8			Default Contactless Application Capabilities

Legend:
M Mandatory.
C Conditional.
¹⁾ qVSDC (Quick VSDC) is an EMV-compliant payment application supported over the contact or contactless interface.

- 2-14.5.8.3 A For the Identifier '000A', the command shall only be sent, if the transaction is token based, i.e. the Card Data Source was '03' during the *Initiate Payment* command. The command shall be sent after the response to the *Validate Data* command has been received and before the *Complete Payment* command is issued.

NOTE: An unsuccessful response will return an ASW1-ASW2 = '10F5' (Identifier not allowed for this transaction).

- 2-14.5.8.4 A For the Identifier '000B', the command shall only be sent, if the transaction is an EMV transaction, and the cards is present, i.e. the Card Data Source was '00' during the *Initiate Payment* command. The command shall be sent after the response to the *Complete Payment* command has been received and before a new transaction is initiated.

NOTE: An unsuccessful response will return an ASW1-ASW2 = '10F5' (Identifier not allowed for this transaction).

- 2-14.5.8.5 A For the Identifier '000D', the command shall only be sent, if the transaction is an online transaction. The command shall be sent after the response to the *Validate Data* command has been received and before the *Complete Payment* command is issued. Null data will be returned, if the information was not received from the host.
- NOTE:** This command is only useful for certain regions. See the different regional requirements in section 1-15.
- 2-14.5.8.6 A For the Identifier '000E', the command shall only be sent, if the transaction is an Authorization Request. The command shall be sent after the response to the *Validate Data* command has been received and before the *Complete Payment* command. The command will return an ASW = '10CA' if no amount information was returned from the host.
- NOTE:** This command is only useful for certain regions. See the different regional requirements in section 1-15.
- 2-14.5.8.7 A For the Identifier '000F', the command is mandatory if Card Data Protection or Online PIN for Private Label Cards are supported.
- 2-14.5.8.8 A For the Identifier '0010', the bit "Extended Issuer Envelope" in the Terminal Settings must be set before the command can be issued. The command shall be sent after the *Validate Data* command and before the *Complete Payment* command. The command will return null data if the terminal did not go online or if no data was returned from the host.
- 2-14.5.8.9 A For the Identifier '0012' data elements for all three tracks shall always be present. Non-existing tracks shall be represented with an enciphered block of 8 bytes ([Rndx (4 bytes) || '80 00 00 00']KSES_{CDP}).
- NOTE:** Rndx indicates the random number including the track no in question, see requirement 2-14.5.8.10.
- 2-14.5.8.10 A For the Identifier '0012' the data element Rnd shall be generated in the following way:
- In order to protect the Track2 data element against substitution/removal the Rnd1, Rnd2, Rnd3 are based on the same random number (the 30 MSBits are the same for the three random numbers). The 2 LSBits of the random numbers specifies the track number (Rnd1 = B'xxxx...01', Rnd2 = B'xxxx...10', Rnd3 = B'xxxx...11').
- 2-14.5.8.11 C For the identifier '0012' the command may be issued at any time after the start-up of the terminal. The command is intended to be used after the cardholder has swiped the card and before a transaction is initiated.

Table 2-14.38 - Data elements returned in LEN_{PROPERTY} in the response to the *Get Contactless AID related Information* command

Field	Value	Length (bytes)
LEN _{AID}	Length of AID	1
AID	Application Identifier	5-16
Card Name	Default Card Name linked to the AID	16
Default Kernel ID	Default Kernel Identifier (byte 1 of tag '9F2A')	1
CURR _{ICC}	Currency Code and Currency exponent	3
Default Reader Limit Set	Reader Contactless Floor Limit (Default reader Limit Set)	4
	Reader CVM Required Limit (Default reader Limit Set)	4
	Reader Contactless Transaction Limit (Default reader Limit Set)	4
CURR _{ALT}	Alternative Currency Code and Currency exponent	3
Default Reader Limit Set _{ALT}	Reader Contactless Floor Limit (Alternative Default Reader Limit Set)	4
	Reader CVM Required Limit (Alternative Default Reader Limit Set)	4
	Reader Contactless Transaction Limit (Alternative Default Reader Limit Set)	4
Contactless Terminal Settings	Terminal specific settings	4
TTQ	Terminal Transaction Qualifiers (Tag '9F66')	4
TAC _{DENIAL}	Terminal Action Code - Denial	5
TAC _{ONLINE}	Terminal Action Code - Online	5
TAC _{DEFAULT}	Terminal Action Code - Default	5
MCC	Merchant Category Code (Tag '9F15')	2
TCC	Transaction Category Code (Tag '9F53')	1
Acquirer Identifier	Default Acquirer Identifier (Tag '9F01')	6
Acquirer Name	Default Acquirer Name	24
ME-No	Default Merchant Establishment No	24
Magstripe Indicator	Handling of magstripe transactions	1

Table 2-14.38 - Data elements returned in $LEN_{PROPERTY}$ in the response to the *Get Contactless AID related Information* command (*concluded*)

Field	Value	Length (bytes)
n x Contactless Reader Limits sets (reserve place for minimum 4 sets)		
CNT_{CRL}	Number of Contactless Reader Limits sets in the response. The following Contactless Reader Limits are repeated CNT_{CRL} times	1
LEN_{RAPI_n}	Length of Reader Application Program Identifier	1
$RAPI_n$	Reader Application Program Identifier	1-16
CURR	Currency Code and Currency exponent	3
Reader Limit Set _n	Reader Contactless Floor Limit (Reader Limit Set _n)	4
	Reader CVM Required Limit (Reader Limit Set _n)	4
	Reader Contactless Transaction Limit (Reader Limit Set _n)	4
Continuation Indicator	'00' = All AID related information has been retrieved. 'FF' = More AID related information available. Re-issue command to retrieve	1

2-14.5.8.12 A For the Identifier '0019', the bitmap "Scheme Id Bitmap" holds a bit array of 32 elements. Each bit represents a possible Electronic Receipt Company (ERCo). The bit shall be set for all the ERCo's that shall receive data. The bit array shall be non-empty when issuing the command.

2-14.5.8.13 A The response shall be interpreted as shown in table 2-14.39.

Table 2-14.39 - Data elements returned in $LEN_{PROPERTY}$ in the response to the *Retrieve Hash Value* command

Field	Value	Length (bytes)
$LEN_{PROPERTY}$	Length of the properties requested ('00 00' if no Scheme Ids are identified)	2
n x (Scheme Id to hash) blocks		
Scheme Id	Identifies the Electronic Receipt Company by a binary number	1
Algorithm Id	Algorithm used to compute the hash	1
Salt version	Version of the salt used to compute the hash value	1
LEN_{Hash}	Length of Hash Value	1
Hash Value	Hash value computed by the PSAM	Var. (32)

2-14.5.8.14 A For the identifier '0019' the command shall be issued after the response to the *Initiate XXX Payment* command and before the *Complete Payment* command.

2-14.5.8.15 C The command may, for non-contactless commands, as well be issued after the the *Get Amount* command and before the response to the *Initiate XXX Payment* command.

2-14.5.9 Set Debit/Credit Properties

Command Message

- 2-14.5.9.1 A The *Set Debit/Credit Properties* command shall have the format shown in table 2-14.40.

Table 2-14.40 - Command message of the *Set Debit/Credit Properties* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'A0'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Identifier	Identifies the Property / data element to be requested (see table 2-14.42)	2
LEN _{INFO}	Length of the Additional Info ('00' if absent)	1
Additional Info	Present if additional information is required (see table 2-14.42)	Variable
L _e	'00'	1

NOTE: If the Additional Info contains a length field, LEN_{INFO} shall include this field as well

Response Message

A *successful* response to the *Set Debit/Credit Properties* command has the format shown in table 2-14.41.

Table 2-14.41 - Successful response message for the *Set Debit/Credit Properties* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{PROPERTY}	Length of the properties requested ('0000' if absent)	2
Property	Property / Data element (see table 2-14.42)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

Table 2-14.42 - Properties / Data Elements to be Set

Identifier	Property / Data Element	Command		Response	
		Additional Info		Property	
		Data Element	Length	Data Element	Length
'8000'	Issuer Envelope	LEN _I ED	1 ¹⁾	(Empty)	0
		Issuer Envelope Data	0 – 100 ²⁾		
'8001'	Terminal Settings	Terminal Settings	1	(Empty) ³⁾	0
'8002'	Duplicate Transaction Time-out	Duplicate Transaction Time-out	1	(Empty)	0
'8003'	Selectable Kernel Configurations	Selectable Kernel Configurations	30	(Empty)	0
'8004'	Extended Issuer Envelope	LEN _{EI} ED	1 ¹⁾	(Empty)	0
		Extended Issuer Envelope Data	0 – var.		
'8005' – '8FFF'	Reserved for Future Use				

Legend:

The coding of the data elements can be found in section 2-15, "Data Elements".

- 1) LEN_IED/LEN_{EI}ED = '00' will reset the Issuer Envelope Data/Extended Issuer Envelope Data.
- 2) The maximum length of the Issuer Envelope Data is 100 bytes for EMV, 150 bytes for MSC and Key Entered transactions.
- 3) The PSAM will respond with ASW = '10AB' if PTS (Terminal Settings, bit 7) is requested by terminal and supported by the PSAM.

- 2-14.5.9.2 A For the Identifier '8000', the command will **overwrite** the current envelope data. The command shall be sent after the *Initiate Payment* command and before the *Payment* command, if the data are to be included in an Authorisation/Financial Requests. Data available after the *Payment* command will be transferred into the Advice, unless overwritten. Other data to be sent in the Advice shall be written after the *Validate Data* command and before the *Complete Payment* command.

NOTE: The Issuer Envelope and the Extended Issuer Envelope will be cleared after the *Complete Payment* command.

- 2-14.5.9.3 A For the Identifier '8003', the command shall not be sent before the PSAM has finished the Initialization Sequence. The command shall be sent while the terminal is idle, i.e. after the response to the *Complete Payment* command and before the *Initiate Payment* command.

NOTE: The Selectable Kernel Configurations settings will be cleared in the Initialization Sequence of the PSAM.

- 2-14.5.9.4 A For the Identifier '8004', the command will **append** data to the current envelope. the command shall be sent after the *Initiate Payment* command and before the *Payment* command, if the data are to be included in an Authorisation/Financial Requests. Data available after the *Payment* command will be transferred into the Advice, unless modified. Other data to be sent in the Advice shall be written after the *Validate Data* command and before the *Complete Payment* command.

The terminal must set the Extended Issuer Envelope bit in the Terminal Settings before the envelope can be accessed.

2-14.5.10 Get Random Number

The purpose of the *Get Random Number* command is to be able to provide the Terminal/POS with a true random number in a secure way.

Command Message

- 2-14.5.10.1 A The *Get Random Number* command shall have the format shown in table 2-14.43.

Table 2-14.43 - Command message of the *Get Random Number* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'A0'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'05'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Identifier	Identifies the property/data elements to be requested ('0018')	2
L _{DATA}	Variable	2
LEN _{INFO}	Length of Additional Info ('01')	1
LEN _{RANDOM}	Length of requested Random Number (up to 'FF')	1
L _e	'00'	1

Response Message

A *successful* response to the *Get Random Number* command has the format shown in table 2-14.33.

Table 2-14.44 - Successful response message for the *Get Random Number* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{PROPERTY}	Length of the requested data ('0000' if absent)	2
Seed	Seed used to derive the session key KSES _{CDP}	4
[Random Number]	CDP enciphered Random Number as requested ¹⁾	Var.
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

- 1) The data element Random Number consists of Random number (4 bytes) || Random Number requested (Var.) || Padding according to "ISO/IEC 9797", Padding method 2.

2-14.5.11 Get Key Check Value 2

Command Message

The *Get Key Check Value 2* command has the format shown in table 2-14.45.

Table 2-14.45 - Command message of the *Get Key Check Value 2* command

Field	Value	Length (bytes)
Destination Address	'0301' for the User Interface, PIN Pad	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'65'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0015'	2
PSAM Identification		
RID _{PSAM}	RID used by the PSAM Creator	5
ID _{PSAMCREATOR}	Identifier assigned to the PSAM Creator by the owner of the RID	4
ID _{PSAM}	Identifier assigned by the PSAM Creator to the PSAM	4
Key Derivation Data		
RND _{SESS}	Random data generated by the PSAM	4
NT _{PIN}	Transaction Counter for PIN based transactions	4

Response Message

2-14.5.11.1 A A *successful* response to the *Get Key Check Value 2* command shall have the format shown in table 2-14.46.

Table 2-14.46 - Successful response message for the *Get Key Check Value 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0301'	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000D'	2
PED Identification		
ID _{PPCREATOR}	Identifier of the Pin Pad Creator	4
ID _{PP}	Identifier assigned to the PIN Pad by the PIN Pad Creator	4
KCV _{BSK}	Key Check value for the PED Basic Session Key	3
RC	'0000'	2

2-14.5.12 Get Processing Condition Table

Command Message

- 2-14.5.12.1 A The *Get Processing Condition Table* command from the terminal shall conform to the format defined in table 2-14.47

Table 2-14.47 - Command message for the *Get Processing Condition Table* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0009'	2
CLA	'B0'	1
INS	'3A'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'03'	1
ID _{THREAD}	Thread Identifier	1
Source	'00' = Request the Header '01' = Request the Records	1
Start Location	'00' = Start at first Processing Condition Table entry '01' = Start at next Processing Condition Table entry	1
L _e	'00'	1

Response Messages

- 2-14.5.12.2 A The terminal shall be able to process a *successful* response to the *Get Processing Table* command with the formats as defined in table 2-14.48 and table 2-14.49.
- 2-14.5.12.3 A The terminal shall be able to process an *Approved/Successful - Action Required* short response, with an ASW1 - ASW2 = '10 21'.

Table 2-14.48 - A successful response message for the *Get Processing Condition Table* command (Source = '00' (Header))

Field	Value	Length (bytes)
Destination Address	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Total length of response data	2
TAG _{HEADER}	'E3'	1
LEN _{HEADER}	Length of PCT header	1
TAG _{COUNTRY-CODE}	'9F1A'	2
LEN _{COUNTRY-CODE}	'02'	1
Country Code	Terminal Country Code	2
TAG _{VERSION}	'DF60'	2
LEN _{VERSION}	'02'	1
VERSION _{PCT}	Current PCT version	2
TAG _{SUBVERSION}	'DF61'	2
LEN _{SUBVERSION}	'01'	1
SUBVERSION _{PCT}	Current PCT subversion	1
TAG _{DATE}	'DF62'	2
LEN _{DATE}	'03'	1
DATE _{PCT}	Date of creation (YYMMDD)	3
TAG _{RECORDLEN}	'DF63'	2
LEN _{RECORD}	'01'	1
RECORD _{LENGTH}	Length of each data record in PCT	1
TAG _{RECORDNO}	'DF64'	2

Table 2-14.48 - A successful response message for the *Get Processing Condition Table* command (Source = '00' (Header)) (*concluded*)

LEN _{RECORDNO}	'02'	1
RECORD _{TOTAL}	Total no. of records	2
TAG _{DOL}	'DF6C'	2
LEN _{DOL}	Length of DOL	1
DOL _{DATA}	DOL data, i.e Tag and Length for data in record'	var.
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

Table 2-14.49 - Successful response message for the *Get Processing Condition Table* command (Source = '01' (Body))

Field	Value	Length (bytes)
Destination Ad- dress	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CNT _{RECORDS}	Number of records in this response. The subsequent field is repeated CNT _{RECORDS} times.	1
Records	Contents of the records shall be interpreted according to the Header information (DOL & RECORD _{LENGTH})	var.
Continuation Indicator	'00' = Information for all supported PCT entries retrieved. 'FF' = More PCT entries available. Re-issue command to retrieve.	1
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

Table 2-14.50 - Example of a successful response message to the *Get Processing Condition Table* command (Source = '00' (Header) - Swedish)

Field	Value	Length (bytes)
Destination Address	The PSAM Handler will insert the address of the source of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'003B'	2
TAG _{HEADER}	'E3'	1
LEN _{HEADER}	'38'	1
TAG _{COUNTRY-CODE}	'9F1A'	2
LEN _{COUNTRY-CODE}	'02'	1
Country Code	Terminal Country Code	2
TAG _{VERSION}	'DF60'	2
LEN _{VERSION}	'02'	1
VERSION _{PCT}	Current PCT version	2
TAG _{SUBVERSION}	'DF61'	2
LEN _{SUBVERSION}	'01'	1
SUBVERSION _{PCT}	Current PCT subversion	1
TAG _{DATE}	'DF62'	2
LEN _{DATE}	'03'	1
DATE _{PCT}	Date of creation (YYMMDD)	3
TAG _{RECORDLEN}	'DF63'	2
LEN _{RECORD}	'01'	1
RECORD _{LENGTH}	'14'	1
TAG _{RECORDNO}	'DF64'	2
LEN _{RECORDNO}	'02'	1
RECORD _{TOTAL}	Total no. of records	2
TAG _{DOL}	'DF6C'	2
LEN _{DOL}	'15'	1

Table 2-14.50 - Example of a successful response message to the *Get Processing Condition Table* command (Source = '00' (Header) - Swedish) (*concluded*)

TAG _{PANFROM}	'DF65'	2
LEN _{PANFROM}	'06'	1
TAG _{PANTO}	'DF66'	2
LEN _{PANTO}	'06'	1
TAG _{ACCOUNTTYPE}	'DF67'	2
LEN _{ACCOUNTTYPE}	'01'	1
TAG _{CASHBACK}	'DF68'	2
LEN _{CASHBACK}	'01'	1
TAG _{KEYENTER}	'DF69'	2
LEN _{KEYENTER}	'01'	1
TAG _{BIB}	'DF6A'	2
LEN _{BIB}	'01'	1
TAG _{BIBAMOUNT}	'DF6B'	2
LEN _{BIBAMOUNT}	'04'	1
TAG _{ACQNAME}	'DF6D'	2
LEN _{ACQNAME}	'18'	1
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

NOTE: The order of the data object in the actual DOL may deviate from the order shown above. The DOL in the header specifies the actual order of the data in the data records.

2-14.5.13 PSAM Update

Command Message

- 2-14.5.13.1 A The *PSAM Update* command shall have the format shown in table 2-14.51.

Table 2-14.51 - Command message of the *PSAM Update* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B4'	1
INS	'48' = Clear Data '4A' = Firmware updates '4C' = Encrypted Data '4E' = Encrypted Keys	1
P1, P2	ID _{PSAMAPP} = '8111' or '0011'	2
L _c	Variable	1
ID _{THREAD}	'00'	1
Update Number	b8 – b5 := Segment number of the update b4 – b1 := Total number of segments in this update	1
Tag	Tag identifying data in the update	2
LEN _{UPD}	Length of data in field Update Data	1
Update Data	Update Data. Format is Tag-specific and the total length of this field may exceed the length defined by LEN _{UPD} . The data bytes included may be padded to reach a multiple of 8 bytes.	Variable
S _{UPD}	MAC over the whole command (CLA – Update Data)	8
L _e	'00'	1

Response Message

The response from the PSAM depends on the type of update received. All updates modifying parameters after initialization will return log information. A *successful* response to the *PSAM Update* command without log information has the format shown in table 2-14.52.

Table 2-14.52 - Successful response message for the *PSAM Update* command without log data

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0004'	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

A *successful* response to the *PSAM Update* command with log information has the format shown in table 2-14.53.

Table 2-14.53 - Successful response message for the *PSAM Update* command with log data.

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000D'	2
Event Type	PSAM Update ('01')	1
Tag	Tag identifying the affected data	2
MAC	The MAC of the original Update	8
ASW1-ASW2	Application Status Words	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

NOTE: The indented data after L_{DATA} field are the data to include in a PCI log.

2-14.6 Debit/Credit Transaction Commands

The following sections (2-14.6.1 to 2-14.6.22) detail the commands and responses between the MAD-Handler, PSAM and Merchant Application used during debit/credit transactions.

2-14.6.1 Initiate EMV Payment 2

- 2-14.6.1.1 A This command/response format shall be used if both the terminal and PSAM supports Service Pack. No. 2. For further details, see section 2-8 page 2-8-1, Service Packs.

Command Message

- 2-14.6.1.2 A The *Initiate EMV Payment 2* command shall have the format shown in table 2-14.54.

Table 2-14.54 - Command message of the *Initiate EMV Payment 2* command

Field	Value	Length (bytes)
Destination Ad- dress	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '04' = Contactless. '05' – 'FF' = Reserved for future use	1
LEN _{AID}	Length of AID	1
AID _{EMV}	AID of the selected application	5 – 16
DTHR	Date and time of the transaction	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 20: "EMV ICC Specification")	1
LEN _{FCI}	Length of FCI (starting with '6F' (FCI template))	1
FCI	File Control Information conveyed in the Select response	Variable
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN _{AMOUNTS}	Length of amount related fields ('00' if absent)	1
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4

Table 2-14.54 - Command message of the *Initiate EMV Payment 2* command (*concluded*)

CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type (default '00')	1
L _e	'00'	1

Response Message

A *successful* response to the *Initiate EMV Payment 2* command has the format shown in table 2-14.55.

Table 2-14.55 - Successful response message for the *Initiate EMV Payment 2* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15")	16
STAN	Systems Trace Audit Number	3
DATE _{EFFECTIVE}	Application Effective Date	3
PAN _{SEQUENCE}	Application PAN Sequence Number ('FF' if absent)	1
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number ¹⁾	Up to 10
LEN _{MDOL1}	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD-Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) If the terminal supports Card Data Protection, the PAN returned will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

2-14.6.2 EMV Payment

Command Message

- 2-14.6.2.1 A The *EMV Payment* command shall have the format shown in table 2-14.56.

Table 2-14.56 - Command message of the *EMV Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN _{MDOL1}	Length of the concatenated list of data elements (MDOL1 data)	1
MDOL1 Data	If the MDOL1 data are stored and maintained in the Terminal debit/credit application, the MDOL1 data are given to the PSAM in this command.	Variable
L _e	'00'	1

Response Message

A *successful* response to the *EMV Payment* command has the format shown in table 2-14.57.

Table 2-14.57 - Successful response message for the *EMV Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
ATC	Application Transaction Counter (ATC)	2
LEN _{HREQ}	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN _{MDOL2}	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.3 Validate Data 2

Command Message

- 2-14.6.3.1 A The *Validate Data 2* command shall have the format shown in table 2-14.58.
- 2-14.6.3.2 A If the L_C field exceeds 248 bytes, the MAD-Handler shall deliver the data in two command APDUs (segments).
- 2-14.6.3.3 A In such a command the MAD-Handler shall send the first $L_C = 248$ bytes of data in the first segment.

Table 2-14.58 - Command message of the *Validate Data 2* command

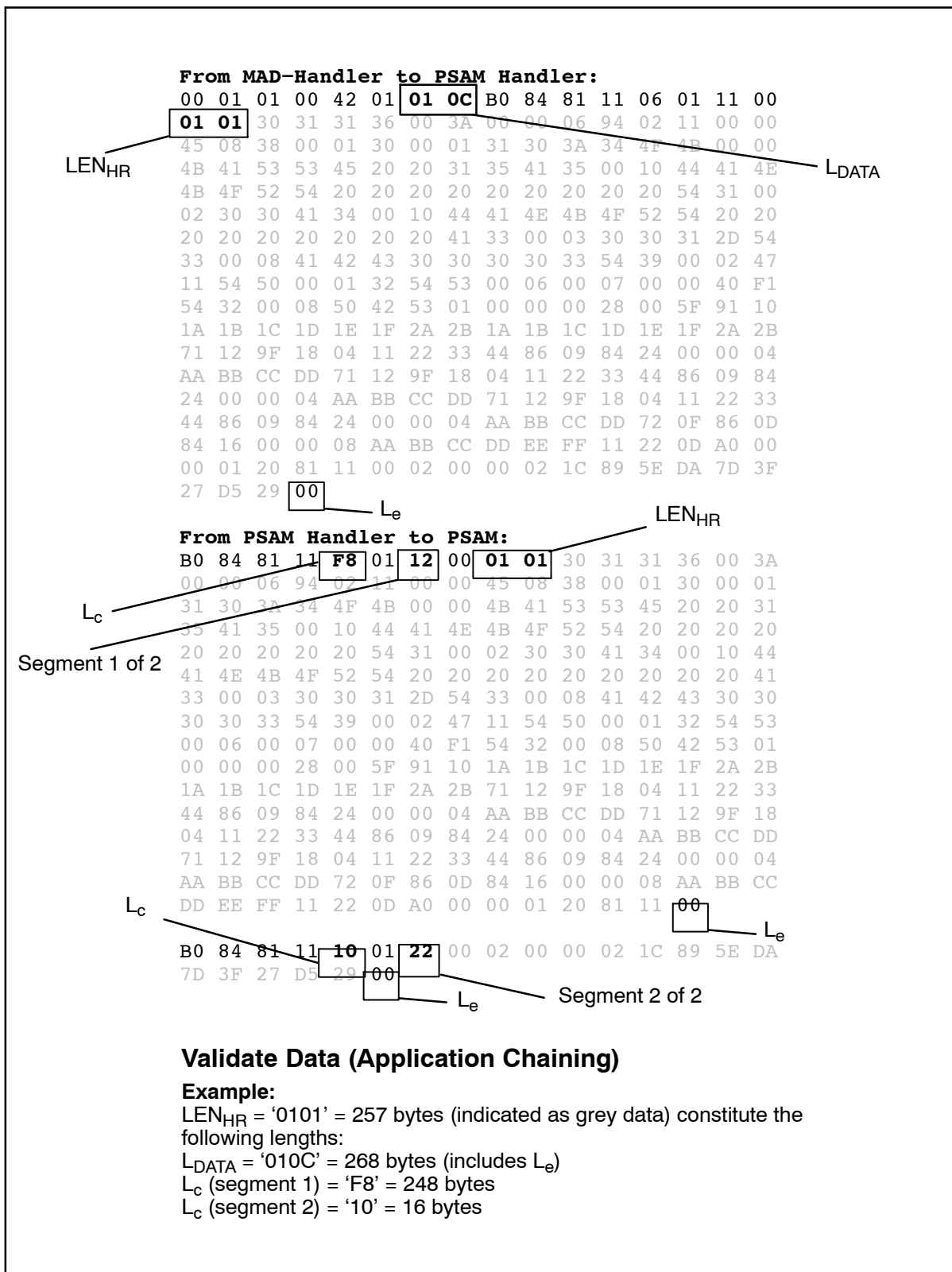
Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'84'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Segment Number	b8 – b5: Segment number of this command b4 – b1: Total number of segments	1
LEN _{MDOL2} ¹⁾	Length of the concatenated list of data elements (MDOL2 data)	1
MDOL2 Data ¹⁾	If the MDOL2 data are stored and maintained in the Terminal EMV Application, the MDOL2 data are given to the PSAM in this command as concatenated data elements (optional)	Variable
LEN _{HR} ¹⁾	Length of host data (if no online connection then equal to '0000')	2
Host Response ¹⁾	Host response data	Variable
L _e	'00'	1

¹⁾ The first (248 - 2 (ID_{THREAD} & Segment Number)) bytes are conveyed in the first segment (segment number 1).

NOTE: If LEN_{MDOL2} is the maximum value of 255 bytes, the Host Response is limited to:
 $246 * 2 - (MDOL2 Data_{MAX} + LEN_{MDOL2} + LEN_{HR})$
 $= 246 * 2 - (255 + 1 + 2) = 234$ bytes

NOTE: See example of the Application Chaining in figure 2-14.1 page 2-14-61

Figure 2-14.1 - Validate Data Command - Application Chaining (Example)



Response Message

A successful response to the *Validate Data 2* command has the format shown in table 2-14.59 and 2-14.60, depending of the segment number or in case of a Prepaid transaction the format shown in table 2-14.61.

Table 2-14.59 - Successful response message for the *Validate Data 2* command (segment *n* of *m*)

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0004'	2
ASW1-ASW2	'0000'	2
RC	'0000'	2

Table 2-14.60 - Successful response message for the *Validate Data 2* command (segment *m* of *m*)

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Action Code-PRINT	Action Code from the acquirer/PSAM	2
Approval Code	Approval Code/Authorization Code (filled with zeroes if absent) ⁵⁾	6
ARC	Authorization Response Code ²⁾ ('0000' if absent)	2
POS Entry Mode	Source of cardholder account data ³⁾	3
CVM Status	Type of CVM and authorization ⁴⁾	1
LEN _{STAN+HREQ}	Length of STAN and host request ('0000' if absent) ¹⁾	2
STAN	Systems Trace Audit Number	3
Host Request	Host request message	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) Host request message and corresponding STAN are present only if the PIN was rejected by the host. PIN retry is only supported when performing MSC transactions with online validation.
- 2) The format of ARC to an2. If no ARC is defined, the value '0000' is returned (e.g. for MSC based transactions).

- 3) The POS Entry Mode returned may differ from the value stated in the *Initiate Payment* command.
- 4) The CVM Status returned may differ from the value stated in the response to the *Payment* command.
- 5) The Approval Code is filled with zeroes ('00 00 00 00 00 00') if no code has been assigned. The terminal may convert and process this specific value as 'spaces', e.g. when printing or logging the information.

Prepaid ICC transactions

- 2-14.6.3.4 A If the following conditions are fulfilled, the terminal shall expect the response given in table 2-14.61:
- The terminal has previously issued a Get Debit/Credit Properties command with the Identifier = '0009'.
 - The transaction is a Prepaid ICC transaction (Card Product Type = Prepaid ICC supported, returned in the response to the Get Debit/Credit Properties command with the Identifier = '0009').
 - The transaction is not a Cancellation transaction (TR □ '06').
 - The transaction is not a Contactless transaction i.e. Card Data Source □ '04'.

Table 2-14.61 - Successful response message for the *Validate Data 2* command (segment *m* of *m*)

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Action Code-PRINT	Action Code from the acquirer/PSAM	2
Approval Code	Approval Code/Authorization Code (filled with zeroes if absent) ⁵⁾	6
ARC	Authorization Response Code ²⁾ ('0000' if absent)	2
POS Entry Mode	Source of cardholder account data ³⁾	3
CVM Status	Type of CVM and authorization ⁴⁾	1
LEN _{STAN+HREQ}	Length of STAN and host request ('0000' if absent) ¹⁾	2
STAN	Systems Trace Audit Number	3
Host Request	Host request message	Variable
LEN _{PREPAID}	Length of the following Prepaid related data ('00' or '22')	1
Initial Card Balance	Card balance <i>before</i> the transaction was initiated ⁶⁾	4
Final Card Balance	Card balance <i>after</i> the actual transaction was completed ⁶⁾	4
Sign _{TOPUP}	Sign of the Top Up Amount ⁶⁾	1
Top Up Amount	Amount transferred from the host account to the card ⁶⁾	4
Sign _{AVAILABLE FUNDS}	Sign of the Available Funds ⁶⁾	1
Available Funds	Amount available on the host account ⁶⁾	4
Maximum Deposit	Maximum amount to deposit on the host account before the legal limit is exceeded ⁶⁾	4
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) Host request message and corresponding STAN are present only if the PIN was rejected by the host. PIN retry is only supported when performing MSC transactions with online validation.
- 2) The format of ARC to an2. If no ARC is defined, the value '0000' is returned (e.g. for MSC based transactions).

- 3) The POS Entry Mode returned may differ from the value stated in the *Initiate Payment* command.
- 4) The CVM Status returned may differ from the value stated in the response to the *Payment* command.
- 5) The Approval Code is filled with zeroes ('00 00 00 00 00 00') if no code has been assigned. The terminal may convert and process this specific value as 'spaces', e.g. when printing or logging the information.
- 6) If an amount is *not* available, the respective field will be set to all 'F's. This rule also applies for the sign fields.

Error Response

Both "short" error responses (as defined in section 2-14.3) or "full-size" responses (according to table 2-14.60) may be returned, when the value of ASW1-ASW2 is greater than or equal to '11 00'.

2-14.6.4 Complete Payment

Command Message

- 2-14.6.4.1 A The *Complete Payment* command shall have the format shown in table 2-14.62.

Table 2-14.62 - Command message of the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	Transaction Status. Coded according to section 2–15: "Data Elements"	1
L _e	'00'	1

Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 2-14.63.

Table 2-14.63 - Successful response message for the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{TOKEN}	Length of the Token ('0000' if absent)	2
TOKEN	Token related data, identifying a consumer card uniquely	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

Application Status Words

2-14.6.5 Initiate MSC Payment 2

Command Message

- 2-14.6.5.1 A The *Initiate MSC Payment 2* command shall have the format shown in table 2-14.64.

Table 2-14.64 - Command message of the *Initiate MSC Payment 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '04' = Contactless. '05'–'FF' = Reserved for future use	1
DTHR	Date and time of the transaction	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 20: "EMV ICC Specification")	1
LEN _{TRACK}	Length of track2 or track3 ¹⁾	1
TRACK DATA	Card data according to POS Entry Mode ¹⁾	Up to 52
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN _{AMOUNTS}	Length of amount related fields ('00' if absent)	1
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type (default '00')	1
L _e	'00'	1

- 1) The PSAM determines whether it is track 2 or track 3 data based on the length of the data. Data less than 19 byte are classified as track 2 while data of exact 52 bytes are classified as track 3.

Response Message

A successful response to the *Initiate MSC Payment 2* command has the format shown in table 2-14.65.

Table 2-14.65 - Successful response message for the *Initiate MSC Payment 2* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15")	16
STAN	Systems Trace Audit Number	3
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number ¹⁾	Up to 10
LEN _{MDOL1}	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD-Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) The PAN returned, is when reading a track3, the concatenated value of PAN Prefix (904x), the real PAN (11 digits) and the PAN Sequence Number (1 digit)

2-14.6.6 Initiate MSC Payment 3

- 2-14.6.6.1 A The command *Initiate MSC Payment 3* shall be used whenever a terminal supports Card Data Protection.

Command Message

- 2-14.6.6.2 A The *Initiate MSC Payment 3* command shall have the format shown in table 2-14.66.

Table 2-14.66 - Command message of the *Initiate MSC Payment 3* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '04' = Contactless. '05'–'FF' = Reserved for future use	1
DTHR	Date and time of the transaction	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 20: "EMV ICC Specification")	1
LEN _{CDP}	Length of Seed □[TrackData] _{KSES_{CDP}}	1
Seed	Seed used to derive the session key KSES _{CDP}	4
[Track Data]	Track Data enciphered by the KSES _{CDP} ¹⁾	Up to 64
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN _{AMOUNTS}	Length of amount related fields ('00' if absent)	1
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type (default '00')	1
L _e	'00'	1

- 1) The data element Track Data consist of Random number (4 bytes) □Track2 (up to 19 bytes) □Padding according to ref. 15: "ISO/IEC 9797", Padding method 2.

Response Message

A *successful* response to the *Initiate MSC Payment 3* command has the format shown in table 2-14.65.

Table 2-14.67 - Successful response message for the *Initiate MSC Payment 3* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15")	16
STAN	Systems Trace Audit Number	3
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number ¹⁾²⁾	Up to 10
LEN _{MDOL1}	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD-Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) The PAN returned, is when reading a track3, the concatenated value of PAN Prefix (904x), the real PAN (11 digits) and the PAN Sequence Number (1 digit)
- 2) The PAN returned will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

2-14.6.7 MSC Payment

Command Message

- 2-14.6.7.1 A The *MSC Payment* command shall have the format shown in table 2-14.68.

Table 2-14.68 - Command message of the *MSC Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN _{MDOL1}	Length of the concatenated list of data elements (MDOL1 data)	1
MDOL1 Data	If the MDOL1 data are stored and maintained in the Terminal debit/credit application, the MDOL1 data are given to the PSAM in this command	Variable
L _e	'00'	1

Response Message

A *successful* response to the *MSC Payment* command has the format shown in table 2-14.69.

Table 2-14.69 - Successful response message for the *MSC Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
LEN _{HREQ}	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN _{MDOL2}	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.8 Complete Payment

Command Message

- 2-14.6.8.1 A The *Complete Payment* command shall have the format shown in table 2-14.70.

Table 2-14.70 - Command message of the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	Transaction Status. Coded according to section 2–15: "Data Elements"	1
L _e	'00'	1

Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 2-14.71.

Table 2-14.71 - Successful response message for the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{TOKEN}	Length of the Token ('0000' if absent)	2
TOKEN	Token related data, identifying a consumer card uniquely	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.9 Initiate Key Entered Payment

Command Message

- 2-14.6.9.1 A The *Initiate Key Entered Payment* command shall have the format shown in table 2-14.72.

Table 2-14.72 - Command message of the *Initiate Key Entered Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '04' = Contactless. '05'–'FF' = Reserved for future use	1
DTHR	Date and time of the transaction	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data, e.g. key-entered	3
TT	Transaction Type (according to ref. 20: "EMV ICC Specification")	1
LEN _{CARDDATA}	Length of key entered data	1
Card Data	PAN □Expiry Date □CV-2	Up to 14
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN _{AMOUNTS}	Length of amount related fields ('00' if absent)	1
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type (default '00')	1
L _e	'00'	1

Response Message

A successful response to the *Initiate Key Entered Payment* command has the format shown in table 2-14.73.

Table 2-14.73 - Successful response message for the *Initiate Key Entered Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15")	16
STAN	Systems Trace Audit Number	3
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN _{MDOL1}	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD-Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.10 Initiate Key Entered Payment 2

- 2-14.6.10.1 A The command *Initiate Key Entered Payment 2* shall be used whenever a terminal supports Card Data Protection.

Command Message

- 2-14.6.10.2 A The *Initiate Key Entered Payment 2* command shall have the format shown in table 2-14.74.

Table 2-14.74 - Command message of the *Initiate Key Entered Payment 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '04' = Contactless. '05'–'FF' = Reserved for future use	1
DTHR	Date and time of the transaction	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data, e.g. key-entered	3
TT	Transaction Type (according to ref. 20: "EMV ICC Specification")	1
LEN _{CDP}	Length of Seed □[CardData] _{KSES_{CDP}}	1
Seed	Seed used to derive the session key KSES _{CDP}	4
[Card Data]	Card Data enciphered by the KSES _{CDP} ¹⁾	Up to 24
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN _{AMOUNTS}	Length of amount related fields ('00' if absent)	1
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type (default '00')	1
L _e	'00'	1

- 1) The data element CardData consist of Random number (4 bytes) □PAN (up to 10 bytes) □Expiry Date (2 bytes) □CV-2 (2 bytes) □Padding according to ref. 15: "ISO/IEC 9797", Padding method 2.

Response Message

A *successful* response to the *Initiate Key Entered Payment 2* command has the format shown in table 2-14.75.

Table 2-14.75 - Successful response message for the *Initiate Key Entered Payment 2* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15")	16
STAN	Systems Trace Audit Number	3
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN _{MDOL1}	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD-Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) The PAN returned will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

2-14.6.11 Key Entered Payment

Command Message

- 2-14.6.11.1 A The *Key Entered Payment* command shall have the format shown in table 2-14.76.

Table 2-14.76 - Command message of the *Key Entered Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN _{MDOL1}	Length of the concatenated list of data elements (MDOL1 data)	1
MDOL1 Data	If the MDOL1 data are stored and maintained in the Terminal debit/credit application, the MDOL1 data are given to the PSAM in this command	Variable
L _e	'00'	1

Response Message

A *successful* response to the *Key Entered Payment* command has the format shown in table 2-14.77.

Table 2-14.77 - Successful response message for the *Key Entered Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
LEN _{HREQ}	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN _{MDOL2}	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.12 Complete Payment

Command Message

2-14.6.12.1 A The *Complete Payment* command shall have the format shown in table 2-14.78.

Table 2-14.78 - Command message of the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	Transaction Status. Coded according to section 2-15: "Data Elements"	1
L _e	'00'	1

Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 2-14.79.

Table 2-14.79 - Successful response message for the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{TOKEN}	Length of the Token ('0000' if absent)	2
TOKEN	Token related data, identifying a consumer card uniquely	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.13 Initiate Token Based Payment 2

Command Message

- 2-14.6.13.1 A The *Initiate Token Based Payment* command shall have the format shown in table 2-14.80.

Table 2-14.80 - Command message of the *Initiate Token Based Payment 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '04' = Contactless. '05' – 'FF' = Reserved for future use	1
DTHR	Date and time of the transaction	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (according to ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 20: "EMV ICC Specification")	1
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN _{AMOUNTS}	Length of amount related fields ('00' if absent)	1
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type	1
L _e	'00'	1

Response Message

A successful response to the *Initiate Token Based Payment 2* command has the format shown in table 2-14.81.

Table 2-14.81 - Successful response message for the *Initiate Token Based Payment 2* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15")	16
STAN	Systems Trace Audit Number	3
LEN _{EMV}	Length of EMV related data ('00' if absent)	1
DATE _{EFFECT.}	Application Effective Date	3
PAN _{SEQUENCE}	Application PAN Sequence Number ('FF' if absent)	1
AID _{EMV}	AID of the selected application	5 – 16
ME _{NUMBER}	Merchant Number	5
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number ¹⁾	Up to 10
LEN _{MDOL1}	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD-Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) If the terminal supports Card Data Protection, the PAN returned will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

2-14.6.14 Token Based Payment

Command Message

- 2-14.6.14.1 A The *Token Based Payment* command shall have the format shown in table 2-14.82.

Table 2-14.82 - Command message of the *Token Based Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN _{MDOL1}	Length of the concatenated list of data elements (MDOL1 data)	1
MDOL1 Data	If the MDOL1 data are stored and maintained in the Terminal debit/credit application, the MDOL1 data are given to the PSAM in this command	Variable
L _e	'00'	1

Response Message

A *successful* response to the *Token Based Payment* command has the format shown in table 2-14.83.

Table 2-14.83 - Successful response message for the *Token Based Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
ATC	Application Transaction Counter (ATC)	2
LEN _{HREQ}	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN _{MDOL2}	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

NOTE: When performing a Supplementary Authorization, the PSAM will initiate a mandatory host request.

NOTE: An ATC value of '0000' indicates that the Application Transaction Counter is not available, which is applicable for Tokens based on magstripe and Key Entered authorizations.

2-14.6.15 Complete Payment

Command Message

2-14.6.15.1 A The *Complete Payment* command shall have the format shown in table 2-14.84.

Table 2-14.84 - Command message of the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	Transaction Status. Coded according to section 2-15: "Data Elements"	1
L _e	'00'	1

Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 2-14.85.

Table 2-14.85 - Successful response message for the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{TOKEN}	Length of the Token ('0000' if absent)	2
TOKEN	Token related data, identifying a consumer card uniquely	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.16 Initiate Contactless Payment

Command Message

2-14.6.16.1 A The *Initiate Contactless Payment* command shall have the format shown in table 2-14.86.

Table 2-14.86 - Command message of the *Initiate Contactless Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '44' = Contactless (ICC), '45' = Contactless (MSD). '05'– 'FF' = Reserved for future use	1
TO	Transaction Options (see table 2-15.35)	1
LEN _{CDP}	Length of Seed [TI, ...Kernel Specific Data] _{KSESCDP}	1
Seed	Seed used to derive the session key KSES _{CDP}	4
[TI	Transaction Identifier (Random number)	4
LEN _{AID}	Length of AID	1
AID	AID of the selected application	5 – 16
DTHR	Date and time of the transaction (YYMMDDHHMM)	5
TR	Transaction Request	1
MI	Merchant Initiative. Parameter(s) forced by the merchant	1
Terminal Ident.	Terminal Identification (Ref. 20: "EMV ICC Specification")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type ('00' = Goods & Services, '09' = Cash-back or '20' Refunds>Returns)	1
LEN _{STAT}	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal (absent)	0
LEN _{AMOUNTS}	Length of amount related fields ('07' or '0B')	1

Table 2-14.86 - Command message of the *Initiate Contactless Payment* command
(concluded)

Field	Value	Length (bytes)
Amount	Amount authorized	4
Amount, Other	Indicates cashback	4 or 0
CURRC	Currency Code	2
CURRE	Currency Exponent	1
Account Type	Account Type (default '00')	1
Batch Number	Batch Number used for reconciliation	12
Error Code	Error Code generated by the kernel	2
Kernel ID	Kernel ID if the external kernel	1
Kernel Version	Kernel Version	2
AI	Action Indicator	2
ATC	Application transaction Counter	2
LEN _{KERNELDATA}	Length of the following Kernel Specific Data	1
Kernel Specific Data]	Kernel Specific Data as requested in the response to the Get Tag List for External Kernel command (in TLV format)	Variable
L _e	'00'	1

NOTE: The data elements [TI ... Kernel Specific Data] consists of Random || TI || ... || Kernel Specific Data || Padding according to ref. 15: ISO/IEC 9797, padding method 2.

NOTE: The data element "Statistics" is currently absent due to limit the number of bytes in the command.

Data elements that candidate for the Kernel Specific Data (requested in the *Get Tag List for External Kernel* command response) can be found in 2-14.87 to 2-14.89. These data are part of the Kernel Specific Data field above and are listed in TLV format.

Table 2-14.87 - payWave Data Elements that candidate for Kernel Specific Data

Tag	Format	Data Element	Comments
5A	cn up to 19 (10)	Primary Account Number	
5F24	n6 (3)	Expiry Date	YYMMDD
5F25	n6 (3)	Application Effective Date	YYMMDD
5F34	n2 (1)	Card Sequence Number/PAN sequence Number	
82	b2 (2)	Application Interchange Profile (AIP)	
8A	an2 (2)	Authorisation Response Code	
9F10	b (up to 32)	Issuer Application Data	
9F1A	n3 (2)	Terminal Country Code	
9F26	b8 (8)	Application Cryptogram	
9F27	b1 (1)	Cryptogram Information Data	
9F34	b3 (3)	CVM Results	
9F37	b4 (4)	Unpredictable Number	
9F41	n4-8 (2-4)	Transaction Sequence Counter (from kernel)	
9F5D	b6 (6)	Available Offline Spending Amount	
9F66	b4 (4)	Terminal Transaction Qualifiers	
9F6E	b4 (4)	Form Factor Indicator	
9F7C	b32 (up to 32)	Customer Exclusive Data	
The maximum number of bytes amount for these candidate data elements is 163 bytes.			

Table 2-14.88 - *PayPass* Data Elements that candidate for Kernel Specific Data (ICC)

Tag	Format	Data Element	Comments
5A	cn up to 19 (10)	Primary Account Number	
5F24	n6 (3)	Expiry Date	YYMMDD
5F25	n6 (3)	Application Effective Date	YYMMDD
5F34	n2 (1)	Card Sequence Number/PAN sequence Number	
82	b2 (2)	Application Interchange Profile (AIP)	
8A	an2 (2)	Authorisation Response Code	
95	b5 (5)	Transaction Verification Results	
9B	b2 (2)	Transaction Status Information	
9F10	b (up to 32)	Issuer Application Data	
9F1A	n3 (2)	Terminal Country Code	
9F26	b8 (8)	Application Cryptogram	
9F27	b1 (1)	Cryptogram Information Data	
9F34	b3 (3)	CVM Results	
9F37	n4 (4)	Unpredictable Number	
9F41	n4-8 (2-4)	Transaction Sequence Counter (from kernel)	
The maximum number of bytes amount for these candidate data elements is 118 bytes.			

Table 2-14.89 - *PayPass* Data Elements that candidate for Kernel Specific Data (MagStripe)

Tag	Format	Data Element	Comments
9F6B	b (up to 19)	Track 2 Data	
The maximum number of bytes amount for these candidate data elements is 22 bytes.			

Response Message

A successful response to the *Initiate Contactless Payment* command has the format shown in table 2-14.90.

Table 2-14.90 - Successful response message for the *Initiate Contactless Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
STAN	Systems Trace Audit Number	3
DATE _{EFFECTIVE}	Application Effective Date	3
PAN _{SEQUENCE}	Application PAN Sequence Number ('FF' if absent)	1
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number. Truncated, leaving the first 6 and last 4 digits	Up to 10
ATC	Application Transaction Counter	2
LEN _{HREQ}	Length of host request ('0000' if offline)	2
Host Request	Host request message	Variable
LEN _{ADD}	Length of additional data ('00' if absent) ¹	1
Action Code-PRINT	Action Code from the acquirer/PSAM	2
Approval Code	Approval Code/Authorization Code (filled with zeroes if absent)	6
ARC	Authorization Response Code ('0000' if absent)	2
POS Entry Mode	Source of cardholder account data	3
CVM Status	Type of CVM and authorization	1
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

NOTE: 1) For online transactions the LEN_{ADD} will be set to '00'. The additional data will be delivered in the response to the *Validate Contactless Payment* command.

2-14.6.17 Validate Contactless Payment

Command Message

- 2-14.6.17.1 A The *Validate Contactless Payment* command shall have the format shown in table 2-14.91.

Table 2-14.91 - Command message of the *Validate Contactless Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'84'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Segment Number	b8 – b5: Segment number of this command b4 – b1: Total number of segments	1
LEN _{HR}	Length of host data (if no online connection then equal to '0000')	2
Host Response ¹⁾	Host response data	Variable
L _e	'00'	1

Response Message

A *successful* response to the *Validate Contactless Payment* command has the format shown in table 2-14.92.

Table 2-14.92 - Successful response message for the *Validate Contactless Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{ADD}	Length of additional data ('0E')	1
Action Code-PRINT	Action Code from the acquirer/PSAM	2
Approval Code	Approval Code/Authorization Code (filled with zeroes if absent)	6
ARC	Authorization Response Code ('0000' if absent)	2
POS Entry Mode	Source of cardholder account data	3
CVM Status	Type of CVM and authorization	1
LEN _{HOSTINFO}	Length of Host Info ('00' or '30')	1
Acquirer Name	Acquirer Name	24
ME-No	Merchant Establishment No	24
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

NOTE: LEN_{HOSTINFO} is equal to '30' only if the host delivers a more precise/different value than the values given in the response to *Get Contactless AID related Information command* concerning the two data elements Acquirer Name or ME-No.

2-14.6.18 Complete Contactless Payment

Command Message

- 2-14.6.18.1 A The *Complete Contactless Payment* command shall have the format shown in table 2-14.93.

Table 2-14.93 - Command message of the *Complete Contactless Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	Transaction Status. Coded according to section 2-15: "Data Elements"	1
TI	Transaction Identifier (Random number if approved else all zeroes)	4
L _e	'00'	1

Response Message

A *successful* response to the *Complete Contactless Payment* command has the format shown in table 2-14.94.

Table 2-14.94 - Successful response message for the *Complete Contactless Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{TOKEN}	Length of the Token ('0000' if absent)	2
TOKEN	Token related data, identifying a consumer card uniquely	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.6.19 Check Stop List

Command Message

The *Check Stop List* command has the format shown in table 2-14.95.

Table 2-14.95 - Command message of the *Check Stop List* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'01'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
LEN _{PAN}	Length of the Primary Account Number	1
PAN	The Primary Account Number ¹⁾	Up to 10

- ¹⁾ If the terminal supports Card Data Protection, the PAN will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

Response Message

- 2-14.6.19.1 A A *successful* response to the *Check Stop List* command shall have the format shown in table 2-14.96.

Table 2-14.96 - Successful response message for the *Check Stop List* command

Field	Value	Length (bytes)
Destination Address	'00pp' The response is sent to the PSAM, which is the originator of the command	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0009'	2
Stop List Status	'00' = Voice Authorization accepted or Card not found in Stop List '01' = Card found in Stop List '02' = Card found in Stop List (pick-up requested) '03' = Stop List not found '04' - '7F' = Reserved for Future Use '80' = Voice Authorization rejected '81' - 'FF' = Reserved for Future Use	1
Approval Code	Approval Code/Authorization Code. If absent filled with spaces (format, see section 2-13)	6
RC	'0000'	2

NOTE: If a successful Voice Authorization is performed, then the terminal should return a StopListStatus of '00'.

Response Codes

The Response Codes (RCs) applicable for the *Check Stop List* command are defined in table 2-14.97.

Table 2-14.97 - Response Codes applicable for the *Check Stop List* command

RC	Meaning	Usage
'0000'	Successful	
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported

2-14.6.20 Verify Signature

Command Message

- 2-14.6.20.1 C The *Verify Signature* command shall have the format shown in table 2-14.98.

Table 2-14.98 - Command message of the *Verify Signature* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0000'	2

Response Message

- 2-14.6.20.2 C A *successful* response to the *Verify Signature* command shall have the format shown in table 2-14.99.

Table 2-14.99 - Successful response message for the *Verify Signature* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0003'	2
Signature Status	'00' = Signature accepted 'FF' = Signature rejected	1
RC	'0000'	2

Response Codes

The Response Codes (RCs) applicable for the *Verify Signature* command are defined in table 2-14.100.

Table 2-14.100 - Response Codes applicable for the *Verify Signature* command

RC	Meaning	Usage
'0000'	Successful	
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported

2-14.6.21 Get Merchant Data

Command Message

The *Get Merchant Data* command has the format shown in table 2-14.101.

Table 2-14.101 - Command message of the *Get Merchant Data* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'04'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0001'	2
Data Requested	'00' = Token related data '01' = Key Entered data '02' - 'FF' = Reserved for Future Use	1

Response Message

- 2-14.6.21.1 A A *successful* response to the *Get Merchant Data* (Token related data is requested) command shall have the format shown in table 2-14.102.
- 2-14.6.21.2 A A *successful* response to the *Get Merchant Data* (Token related data is requested) command shall include the complete Token as delivered in the response to the *Complete Payment* command.

Table 2-14.102 - Successful response message for the *Get Merchant Data* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Data Requested	'00' = Token related data	1
LEN _{DATA}	Length of Token related data	2
Token Data	Token related data	Variable
RC	'0000'	2

Response Codes

The Response Codes (RCs) applicable for the *Get Merchant Data* command are defined in table 2-14.103.

Table 2-14.103 - Response Codes applicable for the *Get Merchant Data* command

RC	Meaning	Usage
'0000'	Successful	
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported

2-14.6.22 Transaction State Information

Command Message

The *Transaction State Information* command has the format shown in table 2-14.104.

Table 2-14.104 - Command message of the *Transaction State Information* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM or '0100' for the MAD-Handler	2
Message Type	'05'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0001'	2
State Information	'00' = Waiting for card '01' = Waiting for application selection '02' = waiting for card validation '03' = Waiting for amount '04' = Waiting for PIN '05' = Waiting for PIN & amount '06' = Waiting (processing) '07' = Waiting for online response '08' - '1F' = Reserved for future use '20' - 'FF' = Proprietary use	1

Response Message

- 2-14.6.22.1 A A successful response to the *Transaction State Information* command shall have the format shown in table 2-14.105.

Table 2-14.105 - Successful response message for the *Transaction State Information* command

Field	Value	Length (bytes)
Destination Address	'00pp' The response is sent to the PSAM, which is the originator of the command or '0100' for the MAD-Handler	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0002'	2
RC	'0000'	2

Response Codes

The Response Codes (RCs) applicable for the *Transaction State Information* command are defined in table 2-14.106.

Table 2-14.106 - Response Codes applicable for the *Transaction State Information* command

RC	Meaning	Usage
'0000'	Successful	
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported

2-14.6.23 Repeat Last ICC Response

Command Message

The *Repeat Last ICC Response* command has the format shown in table 2-14.107.

Table 2-14.107 - Command message of the *Repeat Last ICC Response* command

Field	Value	Length (bytes)
Destination Address	'0202' for the Processor Card Reader	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'06'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0000'	2

Response Message

- 2-14.6.23.1 A A *successful* response to the *Repeat Last ICC Response* command shall have the format shown in table 2-14.108.

Table 2-14.108 - Successful response message for the *Repeat Last ICC Response* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0202' for the Processor Card Reader	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Length of Card Response + '0002'	2
Card Response	Complete R-APDU from card, including the Status Words	Var.
RC	Response Code	2

NOTE: The value of the data elements L_{DATA}, Card Response and RC shall be a copy of the values previously sent in the response to the *ICC Command*.

Response Codes

The Response Codes (RCs) applicable for the *Repeat Last ICC Response*, see Response Codes for the TAPA defined *ICC Command*.

2-14.6.24 Submit Card Reference

Command Message

The *Submit Card Reference* command has the format shown in table 2-14.109.

Table 2-14.109 - Command message of the *Submit Card Reference* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'07'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
Card Reference	Unique Card Reference	8

Response Message

- 2-14.6.24.1 A A *successful* response to the *Submit Card Reference* command shall have the format shown in table 2-14.110.

Table 2-14.110 - Successful response message for the *Submit Card Reference* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0002'	2
RC	'0000'	2

Response Codes

The Response Codes (RCs) applicable for the *Submit Card Reference* command are defined in table 2-14.111.

Table 2-14.111 - Response Codes applicable for the *Submit Card Reference* command

RC	Meaning	Usage
'0000'	Successful	
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF6'	Insufficient resources	The requested operation is valid, but insufficient resources exist to successfully execute the requested function.
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported.
'FFFD'	Transaction interrupt request	Transaction interrupt request: an interrupt indicating that the current transaction shall be terminated gracefully.

2-14.6.25 Submit Card Reference 2

Command Message

The *Submit Card Reference 2* command has the format shown in table 2-14.112.

Table 2-14.112 - Command message of the *Submit Card Reference 2* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'08'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0010'	2
Dual Card Reference	(Set of) Unique Card Reference(s).	16 ¹⁾

- 1) This command is an extension to the *Submit Card Reference* command. The data submitted from the PSAM are two card references. See 2-15.2.53 for detailed information.

Response Message

- 2-14.6.25.1 A A *successful* response to the *Submit Card Reference 2* command shall have the format shown in table 2-14.113.

Table 2-14.113 - Successful response message for the *Submit Card Reference 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0002'	2
RC	'0000'	2

Response Codes

The Response Codes (RCs) applicable for the *Submit Card Reference 2* command are defined in table 2-14.114.

Table 2-14.114 - Response Codes applicable for the *Submit Card Reference 2* command

RC	Meaning	Usage
'0000'	Successful	
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF6'	Insufficient resources	The requested operation is valid, but insufficient resources exist to successfully execute the requested function.
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported.
'FFFD'	Transaction interrupt request	Transaction interrupt request: an interrupt indicating that the current transaction shall be terminated gracefully.

2-14.6.26 Retrieve Card Data MSC

Command Message

The *Retrieve Card Data MSC* command has for a MSC the format shown in table 2-14.115.

Table 2-14.115 - Command message of the *Retrieve Card Data MSC* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'08'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0010'	2
CLA	'B0'	1
INS	'7E'	1
P1.P2	ID _{PSAMAPP} = '8111'	2
L _C	Variable	1
ID _{THREAD}	Thread Identifier of the request	2
Card Data Source	'01' ('00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '44' = Contactless (ICC), '45' = Contactless (MSD), '05'– 'FF' = Reserved for future use)	1
LEN _{ALLTRACKS}	Length of the fields that follows	1
Seed	Seed used to derive the session key KSES _{CDP}	4
LEN _{CDP-TRACK1}	Length of enciphered track 1	1
[Enciph. track1]	Enciphered track 1	Up to 88 ¹⁾
LEN _{CDP-TRACK2}	Length of enciphered track 2	1
[Enciph. Track2]	Enciphered track 2	Up to 24 ¹⁾
LEN _{CDP-TRACK3}	Length of enciphered track 3	1
[Enciph. Track3]	Enciphered track 3	Up to 64 ¹⁾
L _e	'00'	1

- 1) The data element Enciph.Trackx consist of Random number (4 bytes) || Trackx (up to 79) || Padding according to "ISO/IEC 9797", Padding method 2. The same seed is used for all the tracks.

A Private Label card is characterized by;

- Each track will be characterized individually.
- It is, if no ISO PAN is recognized, characterized as a private label card.
- It is, if a ISO PAN is recognized, checked against the MSC table for a Private Label Card bit.
- Clear text will be returned if the card is characterized as a Private Label Card. In all other cases, truncated/ masked PAN will be returned.

Response Message

- 2-14.6.26.1 A A successful response to the *Retrieve Card Data (MSC)* command shall have the format shown in table 2-14.116.

Table 2-14.116 - Successful response message for the *Retrieve Card Data (MSC)* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
Card Service Info (Track 1)	Card Information related to Track 1	1
LEN _{TRACK1}	Length of Track 1 in clear text	1
TRACK1	Track 1 in clear text or with masked data ¹⁾	Up to 76
Card Service Info (Track 2)	Card Information related to Track 2	1
LEN _{TRACK2}	Length of Track 2 in clear text	1
TRACK2	Track 2 in clear text or with masked data ¹⁾	Up to 19
L _{DCR}	Length of Dual Card Reference	1
Dual Card Reference	Two unique card references for Track 2 ²⁾	0 or 16
Card Service Info (Track 3)	Card Information related to Track 3	1
LEN _{TRACK3}	Length of Track3 in clear text	1
TRACK3	Track 3 in clear text or with masked data ¹⁾	Up to 52
Card Name	Official Card Name related to the PAN in track 2 ³⁾	16
ASW1 – ASW2	Application Status Word	2
RC	'0000'	2

1) Data are masked as described in 1-10.10.5. Start sentinel, End sentinel and LRS are omitted.

2) The card references are provided even if the card is identified as a *non* Private Label card.

- 3) The Card Name is present if track2 is recognized by the PSAM, else it is filled with ASCII spaces ('20' '20' ..).

2-14.6.27 Retrieve Card Data ICC

Command Message

The *Retrieve Card Data ICC* command has the format shown in table 2-14.117.

Table 2-14.117 - Command message of the *Retrieve Card Data ICC* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'7E'	1
P1,P2	ID _{PSAMAPP} = '8111'	2
L _C	Variable	1
ID _{THREAD}	Thread Identifier of the request	1
Card Data Source	'00' ('00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token, '44' = Contactless (ICC), '45' = Contactless (MSD), '05'– 'FF' = Reserved for future use)	1
LEN _{FCI}	Length of FCI	1
FCI	File control Information conveyed in the Select response (Starting with '6F' (FCI template))	Var.
Amount	Amount authorized ¹⁾	4
CURRC	Currency Code ¹⁾	2
CURRE	Currency Exponent ¹⁾	1
LEN _{TAGLIST}	Length of the Tag List	1
Tag List	List of tags requested by the terminal ²⁾	Var.
L _e	'00'	1

- 1) Amount and Currency shall be provided to ensure that a request in PDOL for Amount and/or Currency will not halt the command.
- 2) Requesting the tag 'D4' will return the Dual Card Reference (16 bytes). See 2-15.2.53 for detailed information. Fillers in the Tag List will result in the rejection of the command.

Response Message

- 2-14.6.27.1 A A *successful* response to the *Retrieve Card Data ICC* command shall have the format shown in table 2-14.118.

Table 2-14.118 - Successful response message for the *Retrieve Card Data ICC* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable, length of data returned	2
Retrieved Card Data	Retrieved card data as requested by the terminal, in TLV format ¹⁾ . Data may be masked ²⁾ .	Var.
ASW1-ASW2	Application Status Word'	1
RC	'0000'	2

- 1) Requested data not present in the card will be returned with a length of '00'.
- 2) Data for non-Private Label cards will be masked as specified in 1-10.10.5

2-14.6.28 Initiate PIN Entry 2

Command Message

The *Initiate PIN Entry 2* command has the format shown in table 2-14.119.

Table 2-14.119 - Command message of the *Initiate PIN Entry 2* command

Field	Value	Length (bytes)
Destination Address	'0301' for the User Interface, PIN Pad	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'69'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	variable'0010'	2
PSAM Identification		
RID _{PSAM}	RID used by the PSAM Creator	5
ID _{PSAMCREATOR}	Unique identifier of the PSAM Creator	4
ID _{PSAM}	Unique identifier of the PSAM	4
Session Key Derivation Data	Secure Transaction Counter (non-repeating for a given Session Derivation Key) and random data	
RND	Random number ¹⁾	4
NT _{PIN}	PIN Transaction Counter	4
KCV _{BSK}	Current Key Check Value calculated by the PSAM for the PED BSK	3
Min. PIN digits	Minimum number of PIN digits ('04' – '0C')	1
Max. PIN digits	Maximum number of PIN digits ('04' – '0C')	1
Number of PIN entries left	'x0' – 'xE' and 'xF'. The high-order nibble (as indicated by the 'x') is reserved for proprietary coding. The low-order nibble indicates the number of PIN entry attempts that remain. An 'F' in the low-order nibble indicates that this information shall not be displayed.	1
MAC _{IPE}	MAC _{IPE}	8

- 1) The Random number is added to prevent pre-generation of valid KCVs from a genuine PED for later playback to a PSAM.

- 2-14.6.28.1 A The PED shall verify that the PIN Transaction Counter always increase (until a new Session Derivation Key is installed).

Response Message

- 2-14.6.28.2 A A *successful* response to the *Get Amount 3* command shall have the format shown in table 2-14.120.

Table 2-14.120 - Successful response message for the *Initiate PIN Entry 2* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0301' for the User Interface, PIN Pad	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000A'	2
MAC _{IPER}	MAC on the MAC _{IPE} from the command, computed using the KSES _{MAC}	8
NT _{PIN}	PIN Transaction Counter	4
RC	Response code	2

Response Codes

The Response Codes (RCs) applicable for the *Initiate PIN Entry 2* command are defined in table 2-14.124.

Table 2-14.121 - Response Codes applicable for the *Initiate PIN Entry 2* command

RC	Meaning	Usage
'0000'	Successful	
'FFF2'	Time-out	The requested operation is valid, but some external event necessary for the proper execution failed to arrive in time.
'FF8A'	Signature Error	The PED could not verify the KCV received from the PSAM.
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF6'	Insufficient resources	The requested operation is valid, but insufficient resources exist to successfully execute the requested function.
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported

2-14.6.29 Get Amount 3

Command Message

The *Get Amount 3* command has the format shown in table 2-14.122.

Table 2-14.122 - Command message of the *Get Amount 3* command

Field	Value	Length (bytes)
Destination Address	'0400' for the Merchant Application	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'80'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'000B' + LEN _{DD}	2
Timer Flag	'00' = Not timed '80' = Timed	1
Timer	Time-out value in milliseconds	4
Display Message Code	Code indicating the message to be displayed	1
CURR	Currency Code and exponent ('00 00 00' if absent)	3
LEN _{DD}	Length of Discretionary Data	2
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	Primary Account Number ²⁾	Up to 10 ¹⁾
PAN Seq. No.	PAN Sequence Number ('FF' if absent)	1
Amount Request	Amount to be requested '00' = Initial Amount Request (Estimated or Accurate) 'FF' = Final Amount Request (Accurate)	1

- 1) The PAN sent is, when handling track3 data, the concatenated value of PAN Prefix (904x), the real PAN (11 digits) and the PAN Sequence Number (1 digit)
- 2) If the terminal supports Card Data Protection, the PAN returned will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

Response Message

- 2-14.6.29.1 A A *successful* response to the *Get Amount 3* command shall have the format shown in table 2-14.123.

Table 2-14.123 - Successful response message for the *Get Amount 3* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0400' for the Merchant Application	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0010'	2
Transaction Amount	Transaction Amount	4
CURR	Currency Code and exponent	3
LEN _{DD}	'0005' Length of Discretionary Data	2
Amount Other	Amount Other ('00 00 00 00' if absent)	4
Amount Status	Amount delivered '00' = Estimated Amount 'FF' = Accurate Amount	1
RC	'0000'	2

Response Codes

The Response Codes (RCs) applicable for the *Get Amount 3* command are defined in table 2-14.124.

Table 2-14.124 - Response Codes applicable for the *Get Amount 3* command

RC	Meaning	Usage
'0000'	Successful	
'FF40'	Invalid Currency	
'FF41'	Invalid Currency Exponent	
'FFF2'	Time-out	The requested operation is valid, but some external event necessary for the proper execution failed to arrive in time.
'FFF3'	Handler error	Generic message that an unspecified error has occurred
'FFF5'	Handler busy	The Handler received the message but is unable to process it at this moment. The requesting handler must try again later
'FFF6'	Insufficient resources	The requested operation is valid, but insufficient resources exist to successfully execute the requested function.
'FFF7'	Handler must be opened	The Handler is not in open status and therefore cannot perform the requested action
'FFFB'	Unsupported operation	The Handler has received a command or an associated data set that was unrecognized or unsupported

2-14.7 Cancellation

2-14.7.1 Initiate Cancellation Payment

Command Message

- 2-14.7.1.1 A The *Initiate Cancellation Payment* command shall have the format shown in table 2-14.125.

Table 2-14.125 - Command message of the *Initiate Cancellation Payment* Command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'000E'	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'08'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'FF' = Undefined.	1
DTHR	Date and time of the transaction	5
TR	Transaction Request = '06' (Cancellation)	1
L _e	'00'	1

Table 2-14.126 - Successful response message for the *Initiate Cancellation Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
Card Name	Card official name (coded according to ref. 12: "ISO/IEC 8859-15") (Original transaction)	16
STAN	Systems Trace Audit Number	3
STAN _{REF}	Systems Trace Audit Number (Original transaction)	3
DATE _{EFFECTIVE}	Application Effective Date (Original transaction, '000000' if absent)	3
PAN _{SEQUENCE}	Application PAN Sequence Number (Original transaction, 'FF' if absent)	1
DTHR	Date and time of the transaction (Original transaction)	5
LEN _{AID}	Length of AID	1
AID _{EMV}	Application Identifier (Original transaction)	0 or 5 – 16
LEN _{PAN}	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number ¹⁾	Up to 10
LEN _{AMOUNTS}	Length of amount related fields	1
Amount	Amount authorized (Original transaction)	4
Amount, Other	Indicates cashback (Original transaction, if present)	0 or 4
CURRC	Currency Code (Original transaction)	2
CURRE	Currency Exponent (Original transaction)	1
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

- 1) If the terminal supports Card Data Protection, the PAN returned will be truncated according to the Card Scheme rules, i.e. leaving the first 6 and last 4 digits. The remaining digits are replaced by 'A'. The full PAN is still padded with a trailing 'F' for byte boundary alignment if needed.

2-14.7.2 Cancellation Payment

Command Message

- 2-14.7.2.1 A The *Cancellation Payment* command shall have the format shown in table 2-14.127.

Table 2-14.127 - Command message of the *Cancellation Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	Variable	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN _{MDOL1}	Length of the concatenated list of data elements (MDOL1 data)	1
MDOL1 Data	If the MDOL1 data are stored and maintained in the Terminal debit/credit application, the MDOL1 data are given to the PSAM in this command	Variable
L _e	'00'	1

Response Message

A *successful* response to the *Cancellation Payment* command has the format shown in table 2-14.128.

Table 2-14.128 - Successful response message for the *Cancellation Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
ATC	Application Transaction Counter (ATC, '0000' if absent)	2
LEN _{HREQ}	Length of host request ('0000')	2
Host Request	Host request message (absent)	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.7.3 Complete Payment

Command Message

- 2-14.7.3.1 A The *Complete Payment* command shall have the format shown in table 2-14.62.

Table 2-14.129 - Command message of the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'02'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	Transaction Status	1
L _e	'00'	1

Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 2-14.63.

Table 2-14.130 - Successful response message for the *Complete Payment* command

Field	Value	Length (bytes)
Destination Address	'0100' The response is sent to the MAD-Handler, which is the originator of the command	2
Source Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	Variable	2
LEN _{TOKEN}	Length of the Token ('0000' if absent)	2
TOKEN	Token related data, identifying a consumer card uniquely	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.8 Local PIN Commands

2-14.8.1 Load LP Keys Command - Method Number 1

Command Message

The *Load LP Keys* command has the format shown in table 2-14.131.

Table 2-14.131 - Command message of the *Load LP Keys* command

Field	Value	Length (bytes)	
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2	
Source Address	'0100' for the MAD-Handler	2	
Message Type	'42'	1	
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1	
L _{DATA}	'0020'	2	
CLA	'B1'	1	
INS	'00'	1	
P1, P2	ID _{PSAMAPP} = '8111'	2	
L _c	'1A'	1	
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1	
Method Number	'01' (Enciphered)	1	
LEN _{MSCD}	Length of Method Specific Command Data = '0016'	2	
Method Specific Command Data	LP-Key-Chain ('00' - '03')	1	
	'00' = LP-KEK	'01' = LP-PPK	1
	LP-KEK-Version	LP-PPK-Version	1
	[LP-KEK-Data] (enciphered with previous value of same key)	[LP-PPK-Data] (enciphered with the LP-KEK in same key-chain)	16
	Key Check Value	3	
L _e	'00'	1	

- 2-14.8.1.1 A DES encipherment of the Keys shall be performed using ECB mode.

Response Message

- 2-14.8.1.2 A A *successful* response to the *Load LP Keys* command shall have the format shown in table 2-14.132.

Table 2-14.132 - Successful response message for the *Load LP Keys* command

Field	Value	Length (bytes)
Destination Address	'0100' for the MAD-Handler	2
Source Address	'00pp' The response is sent to the PSAM, which is the originator of the command	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000A'	2
Method Number	'01' (Enciphered)	1
LEN _{MSRD}	Length of Method Specific Response Data = '0003'	2
Method Specific Response Data	LP-Key-Chain ('00' - '03')	1
	LP-KEK-Version ('00' - 'FF')	1
	LP-PPK-Version ('00' - 'FF')	1
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.8.2 Local PIN Validation

Command Message

The *Local PIN Validation (Plaintext)* command has the format shown in table 2-14.133.

Table 2-14.133 - Command message of the *Local PIN Validation (Plaintext)* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'001C' or '0023'	2
CLA	'B1'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'16' or '1D'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Method Number	'00' Plaintext PIN Block	1
Min. PIN digits	Minimum number of PIN digits ('04' – '0C')	1
Max. PIN digits	Maximum number of PIN digits ('04' – '0C')	1
Number of PIN tries left	'00' – '0E' = Number of tries left '0F' = Information not available	1
Last PIN incorrect	'00' = Information not available '01' = Last PIN entry was incorrect	1
Timer Flag	'00' = Not timed '80' = Timed	1
Time	Time-out value in milliseconds	4
LEN _{AMOUNT}	Length of amount related fields ('00' if absent)	1
Amount	Transaction Amount	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
LEN _{MSCD}	Length of Method Specific Command Data = '0008'	2
Method Specific Command Data	Plaintext PIN Block	8
L _e	'00'	1

2-14.8.2.1

A LEN_{AMOUNT} shall either have the value '00' (if absent) or '07' (if present).

Response Message

- 2-14.8.2.2 A A *successful* response to the *Local PIN Validation (Plaintext)* command shall have the format shown in table 2-14.134.

Table 2-14.134 - Successful response message for the *Local PIN Validation (Plaintext)* command

Field	Value	Length (bytes)
Destination Address	'0100' for the MAD-Handler	2
Source Address	'00pp' The response is sent to the PSAM, which is the originator of the command	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0007'	2
Method Number	'00' (Plaintext PIN Block)	1
LEN _{MSRD}	'0000' Length of Method Specific Response Data	2
Method Specific Response Data	(No specific response data)	0
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

Command Message

The *Local PIN Validation (Enciphered)* command has the format shown in table 2-14.135.

Table 2-14.135 - Command message of the *Local PIN Validation (Enciphered)* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'002E' or '0035'	2
CLA	'B1'	1
INS	'80'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'28' or '2F'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Method Number	'01' (Enciphered PIN Block)	1
Min. PIN digits	Minimum number of PIN digits ('04' – '0C')	1
Max. PIN digits	Maximum number of PIN digits ('04' – '0C')	1
Number of PIN tries left	'00' – '0E' = Number of tries left '0F' = Information not available	1
Last PIN incorrect	'00' = Information not available '01' = Last PIN entry was incorrect	1
Timer Flag	'00' = Not timed '80' = Timed	1
Time	Time-out value in milliseconds	4
LEN _{AMOUNT}	Length of amount related fields ('00' if absent)	1
Amount	Transaction Amount	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
LEN _{MSCD}	Length of Method Specific Command Data = '001A'	2
Method Specific Command Data	LP-Key-Chain ('00' – '03')	1
	LP-PPK-Version ('00' – 'FF')	1
	Enciphered PIN Data (see table 2-14.136 for further details)	24
L _e	'00'	1

2-14.8.2.3 A LEN_{AMOUNT} shall either have the value '00' (if absent) or '07' (if present).

2-14.8.2.4 A The Enciphered PIN Data shall have the format shown in table 2-14.136.

Table 2-14.136 - Coding of the Enciphered PIN Data

Field	Value	Length (bytes)
Enciphered PIN Data (before encipherment)	Random Pad Pattern generated by the entity computing the Enciphered PIN Data	4
	Transaction Counter ('00 00 00 00 causes no verification and incrementation of Transaction Counter by PSAM)	4
	Plaintext PIN Block as defined for Method Number 0	8
	Padding '80 00 00 00 00 00 00 00'	8

- 2-14.8.2.5 A DES encipherment of the data listed in table 2-14.136 shall be performed using CBC mode.

Response Message

- 2-14.8.2.6 A A *successful* response to the *Local PIN Validation (Enciphered)* command shall have the format shown in table 2-14.137.

Table 2-14.137 - Successful response message for the *Local PIN Validation (Enciphered)* command

Field	Value	Length (bytes)
Destination Address	'0100' for the MAD-Handler	2
Source Address	'00pp' The response is sent to the PSAM, which is the originator of the command	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000B'	2
Method Number	'01' (Enciphered PIN Block)	1
LEN _{MSRD}	Length of Method Specific Response Data = '0004'	2
Method Specific Response Data	Transaction Counter as indicated in the command	4
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

2-14.9 Card Data Protection

2-14.9.1 Load Card Data Protection Keys

Command Message

The *Load Card Data Protection Keys* command has the format shown in table 2-14.138.

Table 2-14.138 - Command message of the *Load Card Data Protection Keys* command

Field	Value	Length (bytes)
Destination Address	'00pp' where pp is the sub-address assigned to the PSAM	2
Source Address	'0100' for the MAD-Handler	2
Message Type	'42'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'001D'	2
CLA	'B2'	1
INS	'00'	1
P1, P2	ID _{PSAMAPP} = '8111'	2
L _c	'18'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
Key Type	'00' = KEK _{CDP} , '01' = KEY _{CDP}	1
VK _{KEK}	Key version of the KEK _{CDP,INI} /KEK _{CDP} ('00' = KEK-CDP,INI)	1
VK	Key version of this key ('00' = KEK _{CDP,INI})	1
ALG	Algorithm indicating the method of derivation ('00')	1
[KEY]	Enciphered key to be loaded	16
KCV	Key Check Value computed on clear text key	3
L _e	'00'	1

- 2-14.9.1.1 A 3DES encipherment of the Keys shall be performed using ECB mode for ALG = '00'.

Response Message

- 2-14.9.1.2 A A *successful* response to the *Load Card Data Protection Keys* command shall have the format shown in table 2-14.139.

Table 2-14.139 - Response message for the *Load Card Data Protection Keys* command

Field	Value	Length (bytes)
Destination Address	'0100' for the MAD-Handler	2
Source Address	'00pp' The response is sent to the PSAM, which is the originator of the command	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'0008'	2
VK _{KEK}	Key Version ('FF' if key is absent)	1
KCV _{KEK}	Key Check Value ('00 00 00' if key is absent)	3
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

NOTE: The Key Version (VK_{KEK}) and Key Check Value (KCV_{KEK}) are returned independently of whether the response is successful or not.

2-14.10 ASW1-ASW2 Coding

The PSAM will use the Application Status Words in the response from the PSAM to indicate the nature of an error, or to request that the terminal perform a particular set of actions.

The ASW1-ASW2 codes defined in table 2-14.143 indicate that the command was processed successfully. In this case, the response to the command will contain all defined response data. All other ASW1-ASW2 codes indicate an error response, and only the ASW1-ASW2 is present in the response.

The remaining tables in this section define ASW1-ASW2 codes and any required or recommended terminal actions associated with these codes.

NOTE: ASW1-ASW2 values not assigned in the following tables are reserved for future use.

Table 2-14.140 - TAPA defined ASW1-ASW2

ASW1	ASW2	Meaning
'00'	'00'	Successful
	all other	Reserved for Future Use
'01'	'00'	Reserved for Future Use
'02'	'00'	No information given
	'01'	Application not supported
	'02'	Function not supported
	'03'	PIN Pad is unresponsive
	'04'	PIN Pad unable to synchronize
	all other	Reserved for Future Use
'03' – '0F'	all	Reserved for Future Use
'1x'	all	Application-specific ASW1-ASW2s
'20' – '60'	all	Reserved for Future Use
'61' – '6F'	all	Reserved for conveying SW1 SW2 as received from the Processor Card Reader
'70' – '90'	all	Reserved for Future Use
'91' – '9F'	all	Reserved for conveying SW1 SW2 as received from the Processor Card Reader
'A0' – 'FF'	all	Reserved for Future Use

2-14.10.1 Application Specific ASW1-ASW2 Coding (Debit/Credit)

Application Status Words (ASW1-ASW2) are grouped in categories depending of which action to take. Table 2-14.141 gives the ranges for each category.

Table 2-14.141 - ASW1-ASW2 grouping

Category	ASW1-ASW2
Approved/Successful	'0000'
Approved/Successful – Action requested	'10XX' ¹⁾
Error – Action requested	'11XX'
Declined (Card/Host/PSAM)	'12XX'
	'13XX'
Declined, try again with other parameters	'14XX'
Declined – Pick up	'15XX'
Failed – Retry	'16XX'
Failed – No retry	'17XX'
Contactless –Error/Decline/Fail – Retry	'18XX'
Reserved	'19XX'
RC related (Card Handler)	'1AXX'
RC related (User Interface Handler)	'1BXX'
RC related (Merchant Application Handler)	'1CXX'
RC related (Data Store Handler)	'1DXX'
Reserved	'1EXX'
Local PIN	'1FXX'
Legend:	
1) For the range '10FB' – '10FD', the transaction is not considered successful, but fallback using magnetic stripe technology is allowed.	

2-14.10.1.1 A Conversion of Application Status Words to Message Codes is given in table 2-14.142.

2-14.10.1.2 A New ASW1-ASW2 not yet defined in the following tables, but inside the ranges given in table 2-14.142, shall be treated in the same way as ASW1-ASW2 already defined inside this range.

When the ASW1-ASW2 are in the range '10FA' - '10FF', the action to be requested is to display a specific text at the Cardholder Display as a guidance for the cardholder.

NOTE: ASW1-ASW2 in this range shall be considered Approved/Successful as the remaining part of the range '10XX'.

NOTE: Note that the table 2-14.157 (Debit/Credit PSAM generated ASW1-ASW2s) is considered as guidelines and may under no circumstances be used for implementation purposes. ASW handling shall always apply to the rules given in section 2-5.16 page 2-5-115, Exception Handling and in particular subsection 2-5.16.1 page 2-5-115, General Rules.

- 2-14.10.1.3 A When ASW1-ASW2 = '10FF' (Incorrect PIN, next CVM selected) is returned, the Message Code '0A' (Incorrect PIN) shall be displayed. This ASW1-ASW2 value is typically returned when PIN validation fails and the terminal/PSAM continues to the next Cardholder Verification Method.
- NOTE:** The Message Code '0E' (Wait) should be displayed simultaneously to indicate that the transaction continues.
- NOTE:** Handling of the ASW1-ASW2 = '10FF' can either be: delaying the succeeding *EMV Payment* command by 6 seconds while displaying "Incorrect PIN" & "Wait" or (if possible) displaying the text above while the terminal simultaneously proceeds by issuing the *EMV Payment* command.
- 2-14.10.1.4 B If the Message Code is 'F3' (Technical Failure), the Application Status Words shall be displayed after the text in the Merchant Display.
- 2-14.10.1.5 B Message Code '94' (Suspected fraud), '8F' (Pick up card), 'F6' (Card blocked) and 'F7' (Refer acquirer) shall only be displayed on the Merchant Display. When '94', '8F', 'F6' or 'F7' is to be displayed on the Merchant Display, Message Code '07' (Declined) shall be displayed on the Cardholder Display.

Table 2-14.142 - ASW1-ASW2 Converted to Message Codes

ASW1–ASW2 Range		Message Code	Text	
From	To		English	Danish ³⁾
'0000'	'0000'	'03'	Approved	Godkendt
'0001'	'0FFF'	'F3'	Technical failure	Teknisk fejl
'1000'	'10FA'	'03'	Approved	Godkendt
'10FB'	'10FB'	'0C'/'12' ¹⁾	Not accepted/Use MAG Stripe	Kan ikke anvendes/Brug magnetkortlæser
'10FC'	'10FC'	'11'	Use Chip Reader	Brug chipkortlæser
'10FD'	'10FD'	'0C'/'12' ¹⁾	Not accepted/Use MAG Stripe	Kan ikke anvendes/Brug magnetkortlæser
'10FE'	'10FE'	'03'	Approved	Godkendt
'10FF'	'10FF'	'0A'	Incorrect PIN	Forkert PIN
'1100'	'11FF'	'0F'	Processing error	Teknisk fejl
'1200'	'121F'	'07'	Declined	Afvist
'1220'	'1220'	'09'	Enter PIN	Indtast PIN
'1221'	'1221'	'0A'	Incorrect PIN	Forkert PIN
'1222'	'1222'	'11'	Use Chip Reader	Brug chipkortlæser
'1223'	'122F'	'0C'	Not accepted	Kan ikke anvendes
'1230'	'123F'	'41'	Invalid card	Ugyldigt kort
'1240'	'124F'	'43'	Expired card	Kort udløbet
'1250'	'125F'	'4D'	Incorrect amount	Forkert beløb
'1260'	'126F'	'70'	Insufficient funds ⁴⁾	Beløb for højt
'1270'	'1274'	'94' ²⁾	Suspected fraud	Mulig svindel
'1275'	'127F'	'E7'	Purchase interrupted	Købet er afbrudt
'1280'	'128F'	'F3'	Technical failure	Teknisk fejl
'1290'	'129F'	'F5'	Limit reached	Maksimum er udnyttet
'12A0'	'12AF'	'FF'	Invalid transaction	Ugyldig transaktion
'12B0'	'12BF'	'F7' ²⁾	Refer acquirer	Ring indløser
'12C0'	'12CF'	'95'	PIN exceeded	For mange PIN forsøg
'12D0'	'12DF'	'F9'	Invalid merchant	Ukendt forretning
'12E0'	'12EF'	'FA'	Card unknown	Kortet er ukendt
'12F0'	'12FF'	'FC'	Card/amount recorded	Kort/beløb noteret
'1300'	'130F'	'FD'	Identical purchase	Identisk køb udført
'1310'	'131F'	'FF'	Invalid transaction	Ugyldig transaktion
'1320'	'13FF'	'F3'	Technical failure	Teknisk fejl

Legend:

1) Message Code '12' shall only be displayed when the requirements stated in section 2–4.17 are fulfilled. Message Code '0C' and '12' should preferably be shown simultaneously, alternatively alternating.

2) For Message Code '94', '8F' and 'F7', see requirement 2–14.10.1.5.

3) For other languages see message codes in the different regional parts of section 2–15.

4) ASW '1016' must not be mapped here due to risk handling at UPT's.

Table 2-14.142 - ASW1-ASW2 Converted to Message Codes (*Continued*)

ASW1-ASW2 Range		Message Code	Text	
From	To		English	Danish
'1400'	'140F'	'0C'	Not accepted	Kan ikke anvendes
'1410'	'141F'	'AF'	Invalid currency	Ugyldig valuta
'1420'	'142F'	'EE'	Insert card again	Indlæs kort igen
'1430'	'14FF'	'F3'	Technical failure	Teknisk fejl
'1500'	'15FF'	'8F ²⁾	Pick up card	Spærret – indrag
'1600'	'162F'	'13'	Try again	Prøv igen
'1630'	'163F'	'40'	System error, retry	Systemfejl prøv igen
'1640'	'164F'	'EE'	Insert card again	Indlæs kort igen
'1650'	'1650'	'F4'	Try again later	Prøv igen om lidt
'1651'	'165F'	'40'	System error, retry	Systemfejl prøv igen
'1660'	'16FF'	'F3'	Technical failure	Teknisk fejl
'1700'	'1701'	'06'	Card error	Kort fejl
'1702'	'1702'	'F3'	Technical failure	Teknisk fejl
'1703'	'171D'	'E7'	Purchase interrupted	Købet er afbrudt
'171E'	'176C'	'42'	Card out of order	Kortet virker ikke
'176D'	'176F'	'F3'	Technical failure	Teknisk fejl
'1770'	'177F'	'FA'	Card unknown	Kortet er ukendt
'1780'	'179F'	'F3'	Technical failure	Teknisk fejl
'17A0'	'17AF'	'FF'	Invalid transaction	Ugyldig transaktion
'17B0'	'17FF'	'F3'	Technical failure	Teknisk fejl
'1800'	'182F'	'F3'	Technical failure	Teknisk fejl
'1830'	'184F'	'11'	Use Chip Reader	Brug chipkortlæser
'1850'	'187F'	'07'	Declined	Afvist
'1880'	'18EF'	'F3'	Technical failure	Teknisk fejl
'18F0'	'18F0'	'03'	Approved	Godkendt
'18F1'	'18F1'	'F3'	Technical failure	Teknisk fejl
'18F2'	'18F2'	'07'	Declined	Afvist
'18F3'	'18F3'	'0C'	Not accepted	Kan ikke anvendes
'18F4'	'18F4'	'41'	Invalid card	Ugyldigt kort
'18F5'	'18F5'	'70'	Insufficient funds	Beløb for højt
'18F6'	'18F6'	'E7'	Purchase interrupted	Købet er afbrudt
'18F7'	'18F7'	'FA'	Card unknown	Kortet er ukendt
'18F8'	'18F8'	'FC'	Card/amount recorded	Kort/beløb noteret
'18F9'	'18FF'	'AF'	Invalid currency	Ugyldig valuta

Table 2-14.142 - ASW1-ASW2 Converted to Message Codes (*Concluded*)

ASW1-ASW2 Range		Message Code	Text	
From	To		English	Danish
'1900'	'1B85'	'F3'	Technical failure	Teknisk fejl
'1B86'	'1B86'	'E7'	Purchase interrupted	Købet er afbrudt
'1B87'	'1BF1'	'F3'	Technical failure	Teknisk fejl
'1BF2'	'1BF2'	'E7'	Purchase interrupted	Købet er afbrudt
'1BF3'	'1C3F'	'F3'	Technical failure	Teknisk fejl
'1C40'	'1C4F'	'AF'	Invalid currency	Ugyldig valuta
'1C50'	'1CF2'	'E7'	Purchase interrupted	Købet er afbrudt
'1CF3'	'FFFF'	'F3'	Technical failure	Teknisk fejl

Legend:

- 1) Message Code '12' shall only be displayed when the requirements stated in section 2–4.17 are fulfilled. Message Code '0C' and '12' should preferably be shown simultaneously, alternatively alternating.
- 2) For Message Code '94', '8F' and 'F7', see requirement 2–14.10.1.5.

Table 2-14.143 - Approved/Successful

ASW1-ASW2	APACS	Meaning	Description
'0000'	0000	Successful	No further action

Table 2-14.144 - Approved/Successful - Action Requested

ASW1-ASW2	APACS	Meaning	Description
'1000'	-	Configuration required	The terminal must configure the PSAM application as part of the start-up processing.
'1001'	-	Install transaction required	The terminal must perform an Install transaction and re-start the PSAM
'1002'	-	Restart required	Prior to sending any new Initiate Transaction commands, the terminal must perform the following actions: · Complete all outstanding transactions · Start-up the PSAM.
'1003'	-	New Data available	This ASW1-ASW2 may be received in the response to e.g. the <i>Start-up PSAM</i> command and PSAM Update command. The terminal shall send the <i>Get Supported AIDs</i> , <i>Get Debit/Credit Properties</i> ('0009') and <i>Get MSC Table</i> commands.
'1010'	0003	Approved (VIP)	-
'1011'	0007	Approved, update ICC	-
'1012'	0060	Approved (National use)	Account service-limit-alarm
'1013'	0061	Approved (National use)	Card service-limit-alarm
'1014'	0063	Approved (National use)	Approved but suspected fraud
'1015'	0064	Approved (National use)	Approved without financial impact
'1016'	0065	Approved (National use)	Approved but not authorized by Issuer
'101F'		Exception rule successful	-
'1020'		No issuer response	-
'1021'		Processing Condition Table (PCT) inconsistent	Processing Condition Table in PSAM is not consistent (missing either header or body)
'1022'		Extended Authorization interrupted	The Extended Authorization has deliberately been interrupted after the Card Reference has been delivered to the terminal.
'1023'		KEY _{CDP} not present	Card Data Protection
'1030'	-	No CVM performed successfully	-
'1031'	-	Offline PIN validation failed	-
'1032'	-	PAN mismatch	Application PAN is not equal to the PAN in Track 2 Equivalent Data
'1033'	-	Requested transaction not found	May be returned when performing Last Transaction Check (Get D/C Properties)
'1034'	-	Format error in host message, offline approved	Despite format error in the host message, the transaction is approved offline
'1035'	-	Amount exceeds offline ceiling	-
'1036'	-	Amount exceeds ceiling	-
'1037'	-	Expiry Check not performed by terminal	Track2 validation
'1038'	-	Service Code not interpreted	Track2 validation

Table 2-14.144 - Approved/Successful - Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'1039'	–	Checksum error	–
'103A'	–	Checksum error – Service Record generated	–
'103F'	–	Statistics data removed due to maximum envelope data	Response to <i>Complete Payment</i> command
'1040'	–	Envelope data exceeds the capability of the PSAM version	May be returned when Identifier = 8000 in the <i>Set Debit/Credit Properties</i> (Issuer Envelope)
'1041'	–	Delivery of data for the envelope is too late	The transaction has passed the point where the data in the envelope could be delivered
'1042'	–	Format error while sending data in the envelope	–
'1043'	–	Service Pack not supported by PSAM	Service Pack No. presented in the Exchange Debit/Credit Static Information exceeds the Service Pack(s) supported by the PSAM
'1044'	–	Merchant Application Log failed	It was not possible to store a backup message in the Merchant Application Log
'1057'	–	AIP does not indicate DDA	Contactless
'1058'	–	Mandatory data is missing 1	–
'1059'	–	Redundant data objects (command)	Redundant primitive data objects read in the command
'105A'	–	Thread unknown (soft)	Only applicable for the <i>Complete & Set Debit/Credit Properties</i> command
'105F'	–	Length of modulus does not match Issuer Certificate	–
'1060'	–	Issuer Certificate format error	Certificate Format is not equal to '02'
'1061'	–	Issuer Certificate invalid	–
'1062'	–	Issuer Identification Number mismatch	Issuer Identification Number does not match the relevant part of the PAN
'1063'	–	Card Certificate format error	–
'1064'	–	ICC Certificate PAN mismatch	Recovered PAN is different from Application PAN
'1065'	–	DDOL Tag error	–
'1066'	–	Length of modulus does not match Card Certificate	–
'1067'	–	DAD format error	–
'1068'	–	ICC PIN Certificate PAN mismatch	–
'1069'	–	Missing Signed Dynamic Application Data	Tag '9F4B' not present
'106A'	–	Length of modulus does not match SDA data	–
'106B'	–	SDA/DDA source error	–
'106C'	–	SDA Tag error	–
'106D'	–	SDA format error	–
'106E'	–	AID length error	The length of the AID does not match the expected length for EMV transaction

Table 2-14.144 - Approved/Successful - Action Requested (*continued*)

ASW1-ASW2	APACS	Meaning	Description
'106F'	-	Length of ICC Public Key Modules does not match Signed Dynamic Application Data	
'1070'	-	Issuer Certificate expired	-
'1071'	-	Card Certificate expired	-
'1072'	-	Key mismatch	The PSAMs Certification Authority Public Key Index is not equal to VPKI _{IEP} from card record
'1073'	-	Issuer Certificate algorithm not supported	-
'1074'	-	Issuer Certificate hash algorithm not supported	-
'1075'	-	Issuer Certificate hash result invalid	-
'1076'	-	Card Certificate hash algorithm not supported	-
'1077'	-	Card Certificate algorithm not supported	-
'1078'	-	Card Certificate hash result invalid	-
'1079'	-	DAD hash algorithm not supported	-
'107A'	-	DAD hash result invalid	-
'107B'	-	SDA hash algorithm not supported	-
'107C'	-	SDA hash result invalid	-
'107D'	-	Length of modulus does not match ICC PIN Certificate	-
'107E'	-	ICC PIN Certificate format error	-
'107F'	-	ICC PIN Certificate expired	-
'1080'	-	ICC PIN Certificate invalid	-
'1081'	-	ICC PIN Certificate hash algorithm not supported	-
'1082'	-	ICC PIN Certificate algorithm not supported	-
'1083'	-	ICC PIN Certificate hash result invalid	-
'1084'	-	PIN try counter not readable	Format of the Get Data response is incorrect
'1085'	-	Available Offline Spending Amount not readable	Format of the Get Data response is incorrect
'1086'	-	Length of modulus does not match ICC PKC	
'1087'	-	Script command syntax error	
'1088'	-	TLV error in proprietary record	
'1089'	-	Script Tag error	A tag found in the script that is neither '9F18' nor '86'
'1090'	-	Unpredictable Number missing in CDOL	CDOL1 & CDOL2 (CDA specific)
'1091'	-	Cryptogram Information Data (plaintext & signed) mismatch	CDA specific
'1092'	-	Hash (Signature) wrong	CDA specific
'1093'	-	Hash (Transaction Data) wrong	CDA specific

Table 2-14.144 - Approved/Successful - Action Requested (*continued*)

ASW1-ASW2	APACS	Meaning	Description
'1094'	-	Header/Trailer format error	CDA specific
'1095'	-	Expired Card	Retrieve Card Data command
'10AB'	-	PTS activated	The PSAM acknowledge that PTS is to be used
'10CA'	-	Data not available	Requested data from the host are not available
'10CB'	-	PIN Pad PK record not found	Unable to retrieve the PIN Pad Public Key Record
'10CC'	-	PSAM Certificate error	PIN Pad rejects PSAM Public Key Certificate due to format error
'10CD'	-	Hash algorithm not supported	Indicated hash algorithm not supported by the PIN Pad
'10CE'	-	PSAM PK algorithm not supported	Indicated Public Key algorithm not supported by the PIN Pad
'10CF'	-	Hash result invalid	Hash computed by the PIN Pad is not identical with the hash in certificate
'10D0'	-	RSA key mismatch	VKP _{CA} , PSAM is not recognized
'10D1'	-	PSAM identifier not recognized	PSAM is not known by the PIN Pad
'10D2'	-	Signature error	The signature PS can not be verified
'10D3'	-	PPC Certificate format error	PIN Pad Creator certificate format error
'10D4'	-	PPC Certificate ID mismatch	PIN Pad Certificate ID mismatch
'10D5'	-	PPC Certificate expired	PIN Pad Creator certificate Expired
'10D6'	-	PPC Certificate hash algorithm not supported	PIN Pad Creator certificate hash algorithm not supported
'10D7'	-	PPC Certificate algorithm not supported	PIN Pad Creator certificate algorithm not supported
'10D8'	-	PPC Certificate hash result invalid	PIN Pad Creator certificate hash result invalid
'10D9'	-	PP Certificate format error	PIN Pad certificate format error
'10DA'	-	PP Certificate hash algorithm not supported	PIN Pad certificate hash algorithm not supported
'10DB'	-	PP Certificate ID mismatch	PIN Pad Certificate ID mismatch
'10DC'	-	PP Certificate expired	PIN Pad certificate Expired
'10DD'	-	PP Certificate algorithm not supported	PIN Pad certificate algorithm not supported
'10DE'	-	PP Certificate hash result invalid	PIN Pad Creator certificate hash result invalid
'10DF'	-	PP Certificate Creator ID mismatch	PIN Pad Creator ID mismatch
'10E0'	-	PIN Pad table full	No more PIN Pad entries available
'10E1'	-	Wrong LPKM in certificate record	Length of Public Key modulus not equal to the length of the CA key
'10E2'	-	Wrong record tag in certificate record	-
'10E3'	-	Wrong data length in certificate record	-
'10E4'	-	PIN Pad not synchronized	-
'10E5'	-	Tag error 1	-
'10E6'	-	Tag error 2	-
'10E7'	-	Tag length error 1	-
'10E8'	-	Tag length error 2	-

Table 2-14.144 - Approved/Successful - Action Requested (*concluded*)

ASW1-ASW2	APACS	Meaning	Description
'10E9'	-	ICC and Terminal have different Application Versions	-
'10EA'	-	Requested Service not allowed for card product	-
'10EB'	-	Application not yet effective	-
'10EC'	-	Expired Application	-
'10ED'	-	Identifier not supported	-
'10EE'	-	Wrong input parameter length	-
'10EF'	-	AID not found in AID Table	-
'10F0'	-	PAN not found in MSC Table	-
'10F1'	-	Syntax error (input data)	-
'10F2'	-	Local PIN disabled	Get Debit/Credit Properties
'10F3'	-	Luhn check digit incorrect	-
'10F4'	-	PAN-length not according to table-entry	-
'10F5'	-	Identifier not allowed for this transaction	Get Debit/Credit Properties
'10F6'	-	Unknown Track3	Get Debit/Credit Properties
'10F7'	-	Extended Issuer Envelope not supported according to Terminal Settings	Set Debit/Credit Properties
'10FB'	-	Fallback allowed	See conditions in section 2-4.17
'10FC'	-	Use Chip Reader	Fallback to other technology (Contactless)
'10FD'	-	RFU (Fallback handling)	-
'10FF'	-	Incorrect PIN, next CVM selected	Display message code '0A' "Incorrect PIN" for 6 seconds

Table 2-14.145 - Error - Action Requested

ASW1–ASW2	APACS	Meaning	Description
'1100'	–	Start-up PSAM command required	The terminal must perform the following actions: · Complete all outstanding transactions · Start-up the PSAM.
'1101'	–	Restart required	The terminal must perform the following actions: · Complete all outstanding transactions · Reset (e.g. power off/power on). · Start-up the PSAM
'1110'	–	Outstanding transaction must be completed	Command cannot be performed while transactions are in progress. Terminal must complete all outstanding transactions and resubmit command.
'1111'	–	Command out of sequence	Indicates that the PSAM's "state" for the ID-THREAD is not correct for the command. For example, the ID _{THREAD} in an EMV Payment command must indicate a transaction that has previously been initiated.
'1120'	–	Data incorrect	The data sent in the command from the MAD-Handler were incorrect.
'1121'	–	State error	–
'1122'	–	INS not supported	–
'1123'	–	Chain error	–
'1124'	–	KCV error	–
'1125'	–	Segment no. error	–
'1126'	–	Too many segments	–
'1127'	–	PKx too long	–
'1128'	–	Wrong length for this Tag	–
'1129'	–	Hash error	–
'112A'	–	Parity error	–
'112B'	–	Tag out of range	–
'112C'	–	Syntax error in date	–
'112D'	–	Segment too short	–
'112E'	–	Tag changed between segments	–
'112F'	–	L _c error	The length field L _c does not match the actual length
'1130'	–	LEN _{APDU} error	The length field LEN from the APDU does not match the actual length
'1131'	–	MAC error in command	–
'1132'	–	MDOL2 data present	MDOL2 data is not expected
'1133'	–	MDOL1 data missing	–
'1134'	–	MDOL2 data missing	–
'1135'	–	Counter number out of range	–
'1136'	–	CK _{TOKEN} Key is missing	–
'1137'	–	LEN _{MDOL} error	–
'1138'	–	Cryptogram Information Data (plaintext & signed) mismatch	CDA specific
'1139'	–	Hash (Signature) wrong	CDA specific
'113A'	–	Hash (Transaction Data) wrong	CDA specific

Table 2-14.145 - Error - Action Requested (*continued*)

ASW1-ASW2	APACS	Meaning	Description
'113B'	-	Header/Trailer format error	CDA specific
'1140'	-	Data Store Handler must be opened	The terminal must resolve the problem by sending the Open Handler message to the Data Store Handler.
'1141'	-	Data Store full	Some data must be sent to the acquirer and deleted from the Data Store before processing can be continued.
'1142'	-	Duplicate File IDs	Indicates that there were duplicate file identifiers in the Configure PSAM command. The terminal must provide unique file identifiers for every file.
'1143'	-	Invalid File ID	Indicates that the Data Store Handler Rejected a command for a file identifier originally provided by the terminal in the Configure PSAM command.
'1144'	-	Total Issuer Envelope Data exceeds buffer size	-
'1145'	-	Extended Issuer Envelope not supported according to Terminal Settings	Terminal Settings shall indicate that Extended Issuer Envelope is supported
'1146'	-	Syntax error in Exception Rule Authorization Code	2 nd Check Stop List
'1147'	-	Exception Rule rejected due to the Stop List Status	2 nd Check Stop List
'1150'	-	PSAM deactivated	The PSAM is not in an operational state. The PSAM is irreversible deactivated.
'1151'	-	PSAM busy – Try later	The PSAM resources required to process the command are in use. The terminal may retry the command later.
'1152'	-	Deactivation rejected	Contact the acquirer
'1153'	-	PSAM disabled	-
'1154'	-	Illegal PSAM Life Cycle	-
'1155'	-	Entry number out of range	-
'1156'	-	PSAM not operational	Operational data is missing
'1157'	-	Date older	Date received in the update command is older than the present one in the PSAM
'1158'	-	Thread unknown	Thread does not match the thread issued in the initialize command
'1159'	-	Memory failure	-
'115A'	-	PSAM busy – Active threads	Complete active threads before re-issuing the command
'115B'	-	Version obsolete	The version of the Processing Condition Table is obsolete
'115C'	-	Record length error	The record length of the Processing Condition does not match Update length
'115D'	-	CVM List formatting error	E.g. odd number of bytes
'115F'	-	PTS Tag 9B error	-
'1160'	-	Tag format error	-
'1161'	-	Missing AIP	Application Interchange Profile is missing
'1162'	-	Missing AFL	Application File Locator is missing
'1163'	-	Length of AFL is not a multiple of four	-
'1164'	-	AFL byte error	-

Table 2-14.145 - Error - Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'1165'	–	Tag 70 is missing	Application Elementary File (AEF) Data Template is missing
'1166'	–	Tag 70 length error	Application Elementary File (AEF) Data Template length error
'1167'	–	SFI range error	Short File Identifier is not in the range from 10 to 30.
'1168'	–	Redundant data objects	–
'1169'	–	Mandatory data is missing 2	–
'116A'	–	Tag error 1	–
'116B'	–	Tag error 2	–
'116C'	–	Tag length error 1	–
'116D'	–	Tag length error 2	–
'116E'	–	FCI data is missing	–
'116F'	–	DOL data out of range	–
'1170'	–	Account Type format error	Account Type has not the value 00, 10, 20 or 30
'1171'	–	Timestamp is old	Patch Update (Header & Body)
'1172'	–	FWVersion _{BASE} not found	Patch Update (Header & Body)
'1173'	–	RunVersion _{TARGET} not found	Patch Update (Header)
'1174'	–	FWVersion _{BASE} changed	Patch Update (Header & Body)
'1175'	–	RunVersion _{TARGET} changed	Patch Update (Header & Body)
'1176'	–	Operational Status changed	Patch Update (Header & Body)
'1177'	–	TOTAL _{BODY} out of range	Patch Update (Header)
'1178'	–	Not possible to switch to any operational version	Patch Update (Header & Body)
'1179'	–	Body no. out of range	Patch Update (Body)
'117A'	–	Addresses out of range	Patch Update (Body)
'1180'	–	Mismatch between POS Entry Mode and Card Data Source	–
'1181'	–	Unknown Data Request	Data requested in the <i>Get Merchant Data</i> command are unknown
'1182'	–	Card Data Source error	–
'1183'	–	Card Handler error – No information given	–
'1184'	–	Card Reader must be opened	The terminal must resolve the problem by sending the Open Handler message to the Processor Card Reader.
'1185'	–	Token not expected	The transaction does not allow a token as card data
'1186'	–	Token missing	The transaction requires a token as card data
'1187'	–	Amount missing	The cardholder has not accepted the amount
'1188'	–	Unknown Transaction Type	–
'1189'	–	Track2 missing	–
'118A'	–	Invalid MI request	–
'118B'	–	Authentication error (MAC validation failed)	–

Table 2-14.145 - Error - Action Requested (*continued*)

ASW1-ASW2	APACS	Meaning	Description
'118C'	-	LEN _{STAT} error	-
'118D'	-	Amount format error	-
'118E'	-	Invalid Token Format	-
'118F'	-	Invalid Token	-
'1190'	-	Incorrect padding for encipherment	-
'1191'	-	Mismatch between Token Info and Token Transaction Data	-
'1193'	-	Cash or cashback not supported by the terminal	Additional Terminal Capabilities does not indicate that Cash or cashback is supported
'1194'	-	PSAM Cash functionality not enabled	
'1195'	-	Goods or Services not supported by the terminal	
'1196'	-	Option not supported	Requested option is not supported by the PSAM
'1197'	-	Invalid SW1-SW2 format	SW1-SW2 returned from the card is outside the valid range
'11C0'	-	Wrong PIN Pad ID	-
'11C1'	-	Key Check Value not identical	Synchronization necessary. <i>Start-up PSAM</i> command shall be issued after the <i>Complete Payment</i> command
'11C2'	-	Secure Device not in PIN Entry State	-
'11C3'	-	Termination failed	-
'11C4'	-	Length of modulus does not match	-
'11C5'	-	ICC PIN certificate format error	-
'11C6'	-	ICC PIN certificate expired	-
'11C7'	-	ICC PIN certificate invalid	-
'11C8'	-	ICC PIN certificate hash algorithm not supported	-
'11C9'	-	ICC PIN certificate algorithm not supported	-
'11CA'	-	ICC PIN certificate hash result invalid	-
'11CB'	-	PIN Pad PK record not found	Unable to retrieve the PIN Pad Public Key Record
'11CC'	-	PSAM Certificate error	PIN Pad rejects PSAM Public Key Certificate due to format error
'11CD'	-	Hash algorithm not supported	Indicated hash algorithm not supported by the PIN Pad
'11CE'	-	PSAM PK algorithm not supported	Indicated Public Key algorithm not supported by the PIN Pad
'11CF'	-	Hash result invalid	Hash computed by the PIN Pad is not identical with the hash in certificate
'11D0'	-	RSA key mismatch	VK _{CA, PSAM} is not recognized
'11D1'	-	PSAM identifier not recognized	PSAM is not known by the PIN Pad
'11D2'	-	Signature error	The signature PS can not be verified
'11D3'	-	PPC Certificate format error	PIN Pad Creator certificate format error
'11D4'	-	PPC Certificate ID mismatch	PIN Pad Certificate ID mismatch

Table 2-14.145 - Error - Action Requested (*concluded*)

ASW1–ASW2	APACS	Meaning	Description
'11D5'	–	PPC Certificate expired	PIN Pad Creator certificate Expired
'11D6'	–	PPC Certificate hash algorithm not supported	PIN Pad Creator certificate hash algorithm not supported
'11D7'	–	PPC Certificate algorithm not supported	PIN Pad Creator certificate algorithm not supported
'11D8'	–	PPC Certificate hash result invalid	PIN Pad Creator certificate hash result invalid
'11D9'	–	PP Certificate format error	PIN Pad certificate format error
'11DA'	–	PP Certificate hash algorithm not supported	PIN Pad certificate hash algorithm not supported
'11DB'	–	PP Certificate ID mismatch	PIN Pad Certificate ID mismatch
'11DC'	–	PP Certificate expired	PIN Pad certificate Expired
'11DD'	–	PP Certificate algorithm not supported	PIN Pad certificate algorithm not supported
'11DE'	–	PP Certificate hash result invalid	PIN Pad Creator certificate hash result invalid
'11DF'	–	PP Certificate Creator ID mismatch	PIN Pad Creator ID mismatch
'11E0'	–	PIN Pad table full	No more PIN Pad entries available
'11E1'	–	Wrong LPKM in certificate record	Length of Public Key modulus not equal to the length of the CA key
'11E2'	–	Wrong record tag in certificate record	–
'11E3'	–	Wrong data length in certificate record	–
'11E4'	–	PIN Pad not synchronized	–
'11E5'	–	Unknown state	–
'11E8'	–	Key mismatch (Token)	–
'11E9'	–	Length of modules does not match Token Certificate	–
'11EA'	–	Token Certificate format error	–
'11EB'	–	Token Certificate expired	–
'11EC'	–	Token Certificate hash algorithm not supported	–
'11ED'	–	Token Certificate algorithm not supported	–
'11EE'	–	Token certificate hash result invalid	–
'11EF'	–	CDOL1 error	–
'11F0'	–	CDOL2 error	–
'11F1'	–	TDOL error	–
'11F2'	–	Format error (Generate AC1 response)	–
'11F3'	–	Format error (Generate AC2 response)	–
'11F4'	–	Token length invalid	–
'11F5'	–	Token data hash result invalid	–
'11F6'	–	Length of ICC Public Key Modulus does not match Signed Dynamic Application Data	–

Table 2-14.146 - Declined

ASW1-ASW2	APACS	Meaning	Description
'1200'	1000	No further details	-
'1201'	1004	Restricted card	-
'1202'	1066	National Use	Cancellation cannot be accepted
'1203'	1061	National Use	
'1204'	-	Unknown Action Code	-
'1205'	-	Service is not allowed	-
'1206'	-	Service Code; Card not for international use	-
'1207'	-	Card on Stop List	-
'1208'	-	PI-Card Type not legal for this transaction request	-
'1209'	-	Forced CVM not allowed	-
'120A'	-	CVM not allowed	The requested CVM is not allowed
'120B'	-	Transaction declined by host	-
'120C'	1062	National Use	Unable to locate previous message
'120D'	1063	National Use	Data are inconsistent with original data
'120E'	-	Transaction declined by ICC	ICC returned AAC/AAR
'120F'	-	Voice authorization rejected	
'1210'	-	Cryptogram format error	PSAM request ARQC while ICC returns a TC
'1211'	-	Declined by Terminal/PSAM (TAC-Denial)	Corresponding TVR/TAC-Denial bits
'1212'	-	Declined by Terminal/PSAM (IAC-Denial)	Corresponding TVR/IAC-Denial bits
'1213'	-	Declined by Terminal/PSAM (TAC-Default)	Corresponding TVR/TAC-Default bits
'1214'	-	Declined by Terminal/PSAM (IAC-Default)	Corresponding TVR/IAC-Default bits
'1215'	-	Declined by Terminal/PSAM	E.g. due to mandatory data missing
'1216'	-	Only goods and services are allowed for this card	Position 3 of the Service Code dictates goods and services
'1217'	-	Post registration is not allowed	Either Post Purchase or Post refund is not allowed
'1218'	-	Accumulated Amount – Ceiling exceeded	BankAxept Exception Rule – 2 nd Check Stop List
'1219'	-	Accumulated Amount – Offline Ceiling exceeded	BankAxept Exception Rule – 2 nd Check Stop List
'1220'	1112	PIN data required	-
'1221'	1017/1117	Incorrect PIN	-
'1222'	-	Service Code; ICC to be used	-
'1223'	-	Key Entered transaction not allowed	-
'1224'	-	Fallback is not allowed	-
'1225'	-	Service not allowed	-
'1226'	-	CDA failed	-

Table 2-14.146 - Declined (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'1230'	1064	National Use	Card entry found, but below low–range
'1231'	1065	National Use	PAN–length not according to table–entry
'1232'	1025	Card not effective	–
'1233'	–	Incorrect PAN length	–
'1234'	–	Luhn check digit incorrect	–
'1235'	–	Dankort check digit incorrect	Check digit (modulus 11) relevant for Dankort
'1236'	–	PAN mismatch	Application PAN is not equal to the PAN in Track 2 Equivalent Data
'1237'	–	Track2 Equivalent Data length error	Length exceeds 37 characters
'1240'	1001	Expired card	–
'1241'	1001	ICC Public Key Certificate expired	Certification Expiry Date exceeded
'1250'	1010	Invalid Amount	–
'1260'	1021	Exceeds withdrawal amount limit	–
'1261'		Amount exceeds ceiling	–
'1262'		Amount exceeds offline ceiling	–
'1270'	1002	Suspected fraud	–
'1271'	1029	Suspected counterfeit card	–
'1275'	–	Amount not confirmed/accepted	–
'1276'	–	Transaction interrupted	E.g. power failure
'1277'	–	Extended Authorization terminated	The Extended Authorization has been deliberately terminated after the Card reference has been delivered to the terminal
'1280'	1026	Invalid PIN block	–
'1281'	1027	PIN length error	–
'1282'	1028	PIN key synchronization error	–
'1283'	–	Terminal Action Code (TAC) could not be selected	Parameters not fulfilled (Terminal Type, Terminal Capabilities, Transaction Type etc.)
'1290'	1023	Exceeds withdrawal frequency limit	–
'12A0'		Forced offline not allowed	Request for offline transaction is not accepted by the PSAM
'12A1'		Online transactions not allowed for this Terminal Type	–
'12A2'		Offline transactions not allowed for this Terminal Type	–
'12A3'		Invalid Terminal Type	Exchange Debit/Credit Static Information
'12A4'	1015	Cashback service not available from issuer	Issuer does not support cashback service
'12A5'		Illegal DCC transaction	E.g. zero amount
'12B0'	1003	Card acceptor contact acquirer	–
'12B1'	1005	Card acceptor call acquirers security department	–
'12B2'	1007	Refer to card issuer	
'12B3'	1008	Refer to card issuer's special conditions	
'12B4'	1013	Unacceptable fee	–

Table 2-14.146 - Declined (*concluded*)

ASW1-ASW2	APACS	Meaning	Description
'12B5'	1014	No account of type requested	-
'12B6'		Requested function not supported	-
'12B7'	1016	Not sufficient funds	-
'12B8'	1022	Security violation	-
'12B9'	1060	National Use	Invalid date
'12BA'	0001	Honour with identification	-
'12BB'	0002	Approved for partial amount	-
'12C0'	1006	Allowable PIN tries exceeded	-
'12D0'	1009	Invalid merchant	-
'12E0'	1011	Invalid card number	-
'12E1'	1018	No card record	-
'12E2'	-	Unknown card	AID/PAN does not match the AID list or MSC table
'12E3'	-	AID not supported	The AID in the command is not supported by the PSAM application. The terminal should send the <i>Get Supported AIDs</i> command to retrieve the list of supported AIDs.
'12E4'	-	AID error	The AID does not match the expected AID for EMV transaction
'12E5'	-	Token requires terminal supporting signature	Selectable Kernel Configurations
'12F0'	0062	Loyalty card accepted	Card and amount is recorded
'1300'	1067	National Use	Match on previous transaction
'1310'	1019	Transaction not permitted to cardholder	-
'1311'	1020	Transaction not permitted to terminal	-
'1312'	1024	Violation of law	-
'1313'	-	Supplementary Authorization not allowed	It is not allowed to perform a Supplementary Authorization when the Original/Extended Authorization has been performed offline.
'1314'	-	Cancellation can not be performed (No image)	Either because a Cancellation has been performed or previous transaction can not be cancelled.
'1315'	-	Cancellation can not be performed (Time-out)	
'1316'	-	Cancellation can not be performed (File in Data Store not to be found)	Either because a Cancellation has been performed or previous transaction can not be cancelled.
'1317'	-	Cancellation can not be performed (Advice could not be deleted)	The <i>Delete File Record</i> command was rejected by the Data Store Handler
'1320'	-	External authentication error	External authentication sent to the card was rejected
'1321'	-	No Selectable Kernel Configurations Data	Applicable when No CVM transactions is performed.
'1322'	-	Online transaction required for Cash-back	-
'1323'	-	Transaction Identifier not identical to the one presented previously	Contactless, Complete Contactless Payment

Table 2-14.147 - Declined, try again with other parameters

ASW1–ASW2	APACS	Meaning	Description
'1400'	–	Select other application	The terminal shall eliminate the current application from consideration and return to the application selection to select another application
'1410'	–	Currency not supported	The currency in the command is not supported by the PSAM application.
'1420'	–	Card not present	The terminal may prompt the cardholder to reinsert the card.

Table 2-14.148 - Declined - Pick up

ASW1–ASW2	APACS	Meaning	Description
'1500'	2000	No further details	–
'1501'	2001	Expired card	–
'1502'	2002	Suspected fraud	–
'1503'	2003	Card acceptor contact acquirer	–
'1504'	2004	Restricted card	–
'1505'	2005	Card acceptor call acquirer's security department	–
'1506'	2006	Allowable PIN tries exceeded	–
'1507'	2007	Special conditions	–
'1508'	2008	Lost card	–
'1509'	2009	Stolen card	–
'150A'	2010	Suspected counterfeit card	–
'150B'	–	Card on Stop List, pick-up requested	Merchant is requested to pick-up the card

Table 2-14.149 - Failed - Retry

ASW1–ASW2	APACS	Meaning	Description
'1600'	–	Condition of use not satisfied	This indicates that the pre-requisites to performing a particular action have not been met.
'1601'	5303	Re-enter transaction	–
'1602'	5304	Format error	–
'1603'/'1020'/'1618'	5406 ¹⁾	Cutover in progress	–
'1604'/'1020'	5407 ¹⁾	Card issuer or switch inoperative	–
'1605'	5408	Transaction destination cannot be found for routing	–
'1606'	5409	System malfunction	–
'1607'/'1020'	5410 ¹⁾	Card issuer signed off	–
'1608'/'1020'	5411 ¹⁾	Card issuer timed out	–
'1609'/'1020'	5412 ¹⁾	Card issuer unavailable	–
'160A'	5414	Not able to trace back to original transaction	–
'160B'/'1020'	5415 ¹⁾	Reconciliation cutover or checkpoint error	–
'160C'	5316	MAC incorrect	–
'160D'	5417	MAC key synchronization error	–

Table 2-14.149 - Failed - Retry (*concluded*)

ASW1-ASW2	APACS	Meaning	Description
'160E'	5418	No communication keys available for use	-
'160F'	5419	Encryption key synchronization error	-
'1610'	-	Key Entered data out of range	-
'1611'	5420	Security software/hardware error – try again	-
'1612'	5421	Security software/hardware error – no action	-
'1613'	5423	Request in progress	-
'1614'/'1020'	5445 ¹⁾	Private use	KIR time-out
'1615'	5484	National use	No valid conversion for a field value
'1616'	-	PIN not available	-
'1617'	-	Time-out	-
'1618'	5000	No Host Data received	-
'1619'	-	Illegal Terminal Identification	Contains characters not supported in the 'an' format
'162F'	□□□□□□□□□□ Initial ASW (Reserved for internal use) □□□□□□□□□□		
'1630'	-	Invalid data received	-
'1631'	-	MTI error	-
'1632'	-	Bit map error	Primary Message bitmap is not as expected
'1633'	5304	STAN mismatch	-
'1634'	-	Time mismatch	-
'1635'	-	Date mismatch	-
'1636'	-	GMT offset mismatch	-
'1637'	-	Card Accepting Device mismatch	CAD ID received in the response is different from the CAD ID in the request
'1638'	-	PSAM Identifier error	-
'1639'	-	MAC validation failed	-
'163A'	-	MAD-Handler ID mismatch	MAD-Handler ID echoed is not the same
'163B'	-	Terminal Approval No. mismatch	Terminal Approval No. echoed is not the same
'1640'	-	No response from card	The terminal may attempt to reset the card, or prompt the cardholder to remove and reinsert the card.
'1641'	-	Track2 format error	-
'1642'	-	Track3 format error	-
'1650'	-	All entries in use – New thread cannot be started	The terminal should (re)send the <i>Exchange Debit/Credit Static Information</i> command to determine the maximum number of entries available in the PSAM.
'1651'	-	Fatal error	Entry Number written is higher than the actual number of entries
'1652'	-	Fatal command error	Command not possible to handle
Legend: ¹⁾ For Card Data Source = '00' (EMV), the APACS Action Code is converted to the ASW value '1020' (No issuer response). It is then up to the settings of TVR/TAC/IAC to determine whether the transaction shall proceed off-line or be rejected.			

Table 2-14.150 - Failed - No Retry

ASW1–ASW2	APACS	Meaning	Description
'1700'	–	Card error – No information given	–
'1701'	–	Data not found	Card error
'1702'	–	Previous transaction was not successful	During Start-up, the PSAM recognized an unfinished transaction in the entry
'1703'	–	Transaction declined by merchant/card-holder/terminal	–
'1704'	–	Signature rejected	Signature rejected by merchant
'1705'	–	Goods or services not delivered	Goods or services could not be delivered
'1706'	–	Invalid Transaction Status	Transaction Status not in allowed range
'1707'	–	Complete Payment not expected by PSAM, but performed	–
'176D'	–	Transaction Request illegal	The Transaction Request is not in the legal range
'176E'	–	LEN _{TRACK2} error	–
'1770'	6005	Acquirer not supported by switch	–
'1780'	6002	Invalid transaction	–
'1781'	–	Checksum error – blocked temporary	–
'1782'	–	Checksum error – blocked irreversibly	–
'1783'	–	PSAM set to non-operational after patch update	–
'1784'	–	KEY _{CDP} not present	Card Data Protection (CDP)
'1785'	–	KEY _{CDP} not loaded after Start-up PSAM	Card Data Protection (CDP)
'1786'	–	Decryption error	Card Data Protection (CDP)
'1787'	–	KEK _{CDP} not present	Card Data Protection (CDP)
'1788'	–	Undefined Key Type	Card Data Protection (CDP)
'17A0'	6013	Duplicate transmission	–
'17A1'	6022	Message number out of sequence	–
'17A2'	6050	Violation of business arrangement	–

Table 2-14.151 - Contactless/Loyalty - Technical failure

ASW1–ASW2	APACS	Meaning	Description
'1800'	–	Terminal error	–
'1801'	–	Pre-processing error	–
'1802'	–	PPSE error	–
'1803'	–	Select error	–
'1804'	–	Card present, but power-up fails	–
'1805'	–	Protocol activation error	–
'1806'	–	Terminal missing data	–
'1807'	–	Card not present/card removed	–
'1808'	–	Transaction aborted by application/merchant	–
'1809'	–	Previous transaction not finished	–
'1810'	–	Kernel error	–
'1811'	–	Offline declined	–

Table 2-14.152 - Contactless - Use Chip Reader

ASW1-ASW2	APACS	Meaning	Description
'1812'	-	ICC missing data	-
'1813'	-	ICC redundant data	-
'1814'	-	ICC data format error	-
'1815'	-	Use contact interface	-
'1816'	-	Expired certificate	-
'1817'	-	Revoked certificate	-
'1818'	-	Kernel not available	-
'1819'	-	Communication error	-
'181A'	-	Error in input parameters	-
'181D'	-	Error Code could not be mapped to ASW	-
'181E'	-	Mismatch between Error Code and Action Indicator (AI) value	-
Reserved for local and loyalty cards			
'18F0'	-	Approved	
'18F1'	-	Technical failure	
'18F2'	-	Declined	
'18F3'	-	Not accepted	
'18F4'	-	Invalid card	
'18F5'	-	Insufficient funds	
'18F6'	-	Purchase interrupted	
'18F7'	-	Card unknown	
'18F8'	-	Card/amount recorded	
'18F9'	-	Invalid currency	

Table 2-14.153 - Error Response - RC related (Card Handler)

ASW1–ASW2	APACS	Meaning	Description
'1A21'	–	Output buffer overflow	Card Handler
'1A23'	–	Card did not respond	–
'1A24'	–	No card in reader	–
'1A25'	–	Unrecoverable Transmission Error	–
'1A26'	–	Card buffer overflow	–
'1A27'	–	Unrecoverable Protocol error	–
'1A28'	–	Response has no status words	–
'1A29'	–	Invalid buffer	–
'1A2A'	–	Other card error	–
'1A2B'	–	Card partially in reader	–
'1AF2'	–	Time-out	–
'1AF3'	–	Handler error	–
'1AF4'	–	Handler must be initialized	–
'1AF5'	–	Handler busy	–
'1AF6'	–	Insufficient resources	–
'1AF7'	–	Handler must be opened	–
'1AFB'	–	Unsupported operation	–

Table 2-14.154 - Error Response - RC related (User Interface Handler)

ASW1-ASW2	APACS	Meaning	Description
'1B34'	-	Unknown Message Code	-
'1B35'	-	Code Table not supported	-
'1B80'	-	No KCV available, KSES not present	-
'1B81'	-	Wrong PIN Pad ID	-
'1B82'	-	Authentication Error (MAC validation failed)	-
'1B83'	-	PSAM Identifier not recognized	-
'1B84'	-	Parameters out of range	-
'1B85'	-	Key check values not identical, synchronization necessary	<i>Start-up PSAM command shall be issued after the Complete Payment command</i>
'1B86'	-	PIN not available	-
'1B87'	-	Secure Device not in PIN Entry State	-
'1B88'	-	Termination Failed	-
'1B89'	-	Record not found	-
'1B8A'	-	Signature Error	-
'1B8B'	-	Hash Error	-
'1B8C'	-	PSAM Certificate Error	-
'1B8D'	-	Hash algorithm not supported	-
'1B8E'	-	PSAM PK algorithm not supported	-
'1B8F'	-	Hash result invalid	-
'1B90'	-	RSA key mismatch. VKP _{CA} , PSAM not recognized	-
'1BF2'	-	Time-out	-
'1BF3'	-	Handler error	-
'1BF4'	-	Handler must be initialized	-
'1BF5'	-	Handler busy	-
'1BF6'	-	Insufficient resources	-
'1BF7'	-	Handler must be opened	-
'1BFB'	-	Unsupported operation	-

Table 2-14.155 - Error Response - RC related (Merchant Application Handler)

ASW1-ASW2	APACS	Meaning	Description
'1C40'	-	Invalid Currency	-
'1C41'	-	Invalid Currency Exponent	-
'1CF2'	-	Time-out	-
'1CF3'	-	Handler error	-
'1CF4'	-	Handler must be initialized	-
'1CF5'	-	Handler busy	-
'1CF6'	-	Insufficient resources	-
'1CF7'	-	Handler must be opened	-
'1CFB'	-	Unsupported operation	-
'1CFD'	-	Transaction interrupt request	-

Table 2-14.156 - Error Response - RC related (Data Store Handler)

ASW1-ASW2	APACS	Meaning	Description
'1D51'	-	Invalid File ID	-
'1D52'	-	Record too large	-
'1D53'	-	Search key too large	-
'1D55'	-	File could not be accessed	-
'1D57'	-	File read error	-
'1D58'	-	File write error	-
'1D59'	-	Search key already existing	-
'1DF2'	-	Time-out	-
'1DF3'	-	Handler error	-
'1DF4'	-	Handler must be initialized	-
'1DF5'	-	Handler busy	-
'1DF6'	-	Insufficient resources	-
'1DF7'	-	Handler must be opened	-
'1DFB'	-	Unsupported operation	-

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1)

ASW1-ASW2	Meaning	Commands	S	S	M	F	C	E	I	A	D	P	S	C	V	G	S	G
			Start	Supp	MSC	File	Conf	Exch	Instal	Adden	Deacti	PSAM	Synch	Cre-at	Vali-da	Set	Get	Get
			UP	A	T	Ch	p	ange	l	dum	vate	Update	ronize	SR	ate	D	D	P
				IDs	able	arac	170								in	prop	prop	CT
'00xx'	Successful (TAPA defined)																	
	'0000'	Successful	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'02xx'	(TAPA defined)																	
	'0200'	No information given	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'0201'	Application not supported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'0202'	Function not supported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'0203'	PIN Pad is unresponsive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'0204'	PIN Pad unable to synchronize	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'10xx'	Approved/Successful – Action Requested																	
	'1000'	Configuration required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1001'	Installation required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1002'	Restart required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1003'	New data available	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1010'	Approved (VIP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1011'	Approved, update ICC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1012'	Approved (National use)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1013'	Approved (National use)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1014'	Approved (National use)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1015'	Approved (National use)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1016'	Approved (National use)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1020'	No issuer response	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1021'	Processing Condition Table (PCT) inconsistent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1022'	Extended Authorization interrupted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1023'	KEY _{CDP} not present	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1030'	No CVM performed successfully	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1031'	Offline PIN validation failed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1032'	PAN mismatch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1033'	Requested transaction not found	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1034'	Format error in host message, offline approved	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1035'	Amount exceeds offline ceiling	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1036'	Amount exceeds ceiling	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1037'	Expiry Check not performed by terminal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1038'	Service Code not interpreted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1039'	Checksum error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'103A'	Checksum error – Service Record generated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'103F'	Statistics data removed due to maximum envelope data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1040'	Envelope data exceeds the capability of the PSAM version	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1041'	Delivery of data for the envelope is too late	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S	S	M	F	C	E	I	A	D	P	S	C	V	G	S	G
			t	u	S	l	o	x	n	d	d	S	y	r	a	e	e	e
			a	p	le	n	c	h	s	e	A	u	e	l	d	t	t	
			r	A	h	Ch	ar	a	n	t	a	p	r	o	n	i	z	e
			u	I	D	s												
'1042'	Format error while sending data in the envelope																	
'1043'	Service Pack not supported by PSAM																	
'1044'	Merchant Application Log failed																	
'1057'	AIP does not indicate DDA																	
'1058'	Mandatory data is missing 1																	
'1059'	Redundant data objects (command)																	
'105A'	Thread unknown (soft)																	
'105F'	Length of modulus does not match Issuer Certificate																	
'1060'	Issuer Certificate format error																	
'1061'	Issuer Certificate invalid																	
'1062'	Issuer Identification Number mismatch																	
'1063'	Card Certificate format error																	
'1064'	ICC Certificate PAN mismatch																	
'1065'	DDOL Tag error																	
'1066'	Length of modulus does not match Card Certificate																	
'1067'	DAD format error																	
'1068'	ICC PIN Certificate PAN mismatch																	
'1069'	Missing Signed Dynamic Application Data																	
'106A'	Length of modulus does not match SDA data																	
'106B'	SDA/DDA source error																	
'106C'	SDA tag error																	
'106D'	SDA format error																	
'106E'	AID length error																	
'106F'	Length of ICC Public Key Modules does not match Signed Dynamic Application Data																	
'1070'	Issuer Certificate expired																	
'1071'	Card Certificate expired																	
'1072'	Key mismatch																	
'1073'	Issuer Certificate algorithm not supported																	
'1074'	Issuer Certificate hash algorithm not supported																	
'1075'	Issuer Certificate hash result invalid																	
'1076'	Card Certificate hash algorithm not supported																	
'1077'	Card Certificate algorithm not supported																	
'1078'	Card Certificate hash result invalid																	
'1079'	DAD hash algorithm not supported																	
'107A'	DAD hash result invalid																	
'107B'	SDA hash algorithm not supported																	
'107C'	SDA hash result invalid																	
'107D'	Length of modulus does not match ICC PIN Certificate																	

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T
'107E'	ICC PIN Certificate format error																	
'107F'	ICC PIN Certificate expired																	
'1080'	ICC PIN Certificate invalid																	
'1081'	ICC PIN Certificate hash algorithm not supported																	
'1082'	ICC PIN Certificate algorithm not supported																	
'1083'	ICC PIN Certificate hash result invalid																	
'1084'	PIN try counter not readable																	
'1087'	Script command syntax error																	
'1088'	TLV error in proprietary record																	
'1089'	Script Tag error																	
'1090'	Unpredictable Number missing in CDOL																	
'1091'	Cryptogram Information Data mismatch																	
'1092'	Hash (Signature) wrong																	
'1093'	Hash (Transaction Data) wrong																	
'1094'	Header/Trailer format error																	
'1095'	Expired card																	
'10AB'	PTS activated																	☐
'10B2'	Refer to card issuer																	
'10B3'	Refer to card issuer's special conditions																	
'10CA'	Data not available																☐	
'10CB'	PIN Pad PK record not found																	
'10CC'	PSAM Certificate error																	
'10CD'	Hash algorithm not supported																	
'10CE'	PSAM PK algorithm not supported																	
'10CF'	Hash result invalid																	
'10D0'	RSA key mismatch												☐					
'10D1'	PSAM identifier not recognized												☐					
'10D2'	Signature error												☐					
'10D3'	PPC Certificate format error												☐					
'10D4'	PPC Certificate ID mismatch												☐					
'10D5'	PPC Certificate expired												☐					
'10D6'	PPC Certificate hash algorithm not supported												☐					
'10D7'	PPC Certificate algorithm not supported												☐					
'10D8'	PPC Certificate hash result invalid												☐					
'10D9'	PP Certificate format error												☐					
'10DA'	PP Certificate hash algorithm not supported												☐					
'10DB'	PP Certificate ID mismatch												☐					
'10DC'	PP Certificate expired												☐					
'10DD'	PP Certificate algorithm not supported												☐					
'10DE'	PP Certificate hash result invalid												☐					
'10DF'	PP Certificate Creator ID mismatch												☐					

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p o r t e d A I D s	M S C T a b l e	F i l e C h a r a c t e r i s t i c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - d a t e	G e t D / C P r o p	S e t D / C P r o p	G e t P C T
'10E0'	PIN Pad table full												<input type="checkbox"/>					
'10E1'	Wrong LPKM in certificate record												<input type="checkbox"/>					
'10E2'	Wrong record tag in certificate record												<input type="checkbox"/>					
'10E3'	Wrong data length in certificate record												<input type="checkbox"/>					
'10E4'	PIN Pad not synchronized												<input type="checkbox"/>					
'10E5'	Tag error 1																	
'10E6'	Tag error 2																	
'10E7'	Tag length error 1																	
'10E8'	Tag length error 2																	
'10E9'	ICC and Terminal have different Application Versions																	
'10EA'	Requested Service not allowed for card product																	
'10EB'	Application not yet effective																	
'10EC'	Expired Application																	
'10ED'	Identifier not supported															<input type="checkbox"/>		
'10EE'	Wrong AID length															<input type="checkbox"/>		
'10EF'	AID not found in AID Table															<input type="checkbox"/>		
'10F0'	PAN not found in MSC Table															<input type="checkbox"/>		
'10F1'	Syntax error (input data)															<input type="checkbox"/>		
'10F2'	Local PIN disabled															<input type="checkbox"/>		
'10F3'	Luhn check digit incorrect															<input type="checkbox"/>		
'10F4'	PAN-length not according to table-entry															<input type="checkbox"/>		
'10F5'	Identifier not allowed for this transaction															<input type="checkbox"/>		
'10F6'	Unknown Track3															<input type="checkbox"/>		
'10F7'	Extended Issuer Envelope not supported according to Terminal Settings															<input type="checkbox"/>	<input type="checkbox"/>	
'10FB'	Fallback allowed																	
'10FF'	Incorrect PIN, next CVM selected																	
'11xx'	Error – Action Requested																	
'1100'	Start-up PSAM command required		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1101'	Restart required																	
'1110'	Outstanding transaction must be completed		<input type="checkbox"/>															
'1111'	Command out of sequence		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1120'	Data incorrect		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1121'	State error		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1122'	INS not supported		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1123'	Chain error																	
'1124'	KCV error											<input type="checkbox"/>						
'1125'	Segment no. error											<input type="checkbox"/>						
'1126'	Too many segments											<input type="checkbox"/>						
'1127'	PKx too long											<input type="checkbox"/>						
'1128'	Wrong length for this Tag											<input type="checkbox"/>						

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T
'1129'	Hash error											<input type="checkbox"/>						
'112A'	Parity error											<input type="checkbox"/>						
'112B'	Tag out of range											<input type="checkbox"/>						
'112C'	Syntax error in date											<input type="checkbox"/>						
'112D'	Segment too long											<input type="checkbox"/>						
'112E'	Tag changed between segments											<input type="checkbox"/>						
'112F'	L _c error		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1130'	LEN _{APDU} error		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1131'	MAC error in command											<input type="checkbox"/>						
'1132'	MDOL2 data present																	
'1133'	MDOL1 data missing																	
'1134'	MDOL2 data missing																	
'1135'	Counter number out of range											<input type="checkbox"/>						
'1136'	CK _{TOKEN} Key is missing											<input type="checkbox"/>						
'1137'	LEN _{MDOL} error																	
'1138'	Cryptogram Information Data (plaintext & signed) mismatch																	
'1139'	Hash (Signature) wrong																	
'113A'	Hash (Transaction Data) wrong																	
'113B'	Header/Trailer format error																	
'1140'	Data Store Handler must be opened																	
'1141'	Data Store full																	
'1142'	Duplicate File IDs					<input type="checkbox"/>												
'1143'	Invalid File ID					<input type="checkbox"/>												
'1144'	Total Issuer Envelope Data exceeds buffer size																	
'1145'	Extended Issuer Envelope not supported according to Terminal Settings																	
'1150'	PSAM deactivated		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1151'	PSAM Busy – Try later		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1152'	Deactivation rejected											<input type="checkbox"/>						
'1153'	PSAM disabled											<input type="checkbox"/>						
'1154'	Illegal PSAM Life Cycle		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1155'	Entry number out of range											<input type="checkbox"/>						
'1156'	PSAM not operational		<input type="checkbox"/>															
'1157'	Date older											<input type="checkbox"/>						
'1158'	Thread unknown																	<input type="checkbox"/>
'1159'	Memory failure		<input type="checkbox"/>									<input type="checkbox"/>						
'115A'	PSAM busy – Active threads																	
'115B'	Version obsolete																	<input type="checkbox"/>
'115C'	Record length error																	<input type="checkbox"/>

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - d a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
'115D'	CVM List formatting error																		
'115F'	PTS Tag 9B error								□										
'1160'	Tag format error																		
'1161'	Missing AIP																		
'1162'	Missing AFL																		
'1163'	Length of AFL is not multiple of four																		
'1164'	AFL byte error																		
'1165'	Tag 70 is missing																		
'1166'	Tag 70 length error																		
'1167'	SFI range error																		
'1168'	Redundant data objects																		
'1169'	Mandatory data is missing 2																		
'116A'	Tag error 1																		
'116B'	Tag error 2																		
'116C'	Tag length error 1																		
'116D'	Tag length error 2																		
'116E'	FCI data missing																		
'116F'	DOL data out of range																		
'116F'	DOL data out of range																		
'1170'	Account Type format error																		
'1171'	Timestamp is old																		
'1172'	FWVersion _{BASE} not found																		
'1173'	RunVersion _{TARGET} not found																		
'1174'	FWVersion _{BASE} changed																		
'1175'	RunVersion _{TARGET} changed																		
'1176'	Operational Status changed																		
'1177'	TOTAL _{BODY} out of range																		
'1178'	Not possible to switch to any operational version																		
'1179'	Body no. out of range																		
'117A'	Addresses out of range																		
'1180'	Mismatch between POS Entry Mode and Card Data Source																		
'1181'	Unknown Data Request																		
'1182'	Card Data Source error																		
'1183'	Card Handler error – No information given																		
'1184'	Card Reader must be opened																		
'1185'	Token not expected																		
'1186'	Token missing																		
'1187'	Amount missing																		
'1188'	Unknown Transaction Type																		
'1189'	Track2 missing																		

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U p	S u p p o r t A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - a t e l i n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
'118A'	Invalid MI request																		
'118B'	Authentication error (MAC validation failed)																		
'118C'	LEN _{STAT} error																		
'118D'	Amount format error																		
'118E'	Invalid Token Format																		
'118F'	Invalid Token																		
'1190'	Incorrect padding for encipherment																		
'1191'	Mismatch between Token Info and Token Transaction Data																		
'1193'	Cash or cashback not supported by terminal																		
'1194'	PSAM Cash functionality not enabled																		
'1195'	Goods or Services not supported by the terminal																		
'1196'	Option not supported																		□
'1197'	Invalid SW1-SW2 format																		
'11C0'	Wrong PIN Pad ID																		□
'11C1'	Key Check value not identical																		□
'11C2'	Secure Device not in PIN Entry State																		□
'11C3'	Termination failed																		□
'11C4'	Length of modulus does not match																		
'11C5'	ICC PIN certificate format error																		
'11C6'	ICC PIN certificate expired																		
'11C7'	ICC PIN certificate invalid																		
'11C8'	ICC PIN certificate hash algorithm not supported																		
'11C9'	ICC PIN certificate algorithm not supported																		
'11CA'	ICC PIN certificate hash result invalid																		
'11CB'	PIN Pad PK record not found																		□
'11CC'	PSAM Certificate error																		□
'11CD'	Hash algorithm not supported																		□
'11CE'	PSAM PK algorithm not supported																		□
'11CF'	Hash result invalid																		□
'11D0'	RSA key mismatch																		
'11D1'	PSAM identifier not recognized																		□
'11D2'	Signature error																		□
'11D3'	PPC Certificate format error																		
'11D4'	PPC Certificate ID mismatch																		
'11D5'	PPC Certificate expired																		
'11D6'	PPC Certificate hash algorithm not supported																		
'11D7'	PPC Certificate algorithm not supported																		
'11D8'	PPC Certificate hash result invalid																		
'11D9'	PP Certificate format error																		
'11DA'	PP Certificate hash algorithm not supported																		

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - d a t e	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
'11DB'	PP Certificate ID mismatch																		
'11DC'	PP Certificate expired																		
'11DD'	PP Certificate algorithm not supported																		
'11DE'	PP Certificate hash result invalid																		
'11DF'	PP Certificate Creator ID mismatch																		
'11E0'	PIN Pad table full																		
'11E1'	Wrong LPKM in certificate record																		
'11E2'	Wrong record tag in certificate record																		
'11E3'	Wrong data length in certificate record																		
'11E4'	PIN Pad not synchronized																		
'11E5'	Unknown state																		
'11E6'	State address not found																		
'11E7'	Command address not found																		
'11E8'	Key mismatch (Token)																		
'11E9'	Length of modulus does not match Token Certificate																		
'11EA'	Token Certificate format error																		
'11EB'	Token Certificate expired																		
'11EC'	Token Certificate hash algorithm not supported																		
'11ED'	Token Certificate algorithm not supported																		
'11EE'	Token Certificate hash result invalid																		
'11EF'	CDOL1 error																		
'11F0'	CDOL2 error																		
'11F1'	TDOL error																		
'11F2'	Format error (Generate AC1 response)																		
'11F3'	Format error (Generate AC2 response)																		
'11F4'	Token length invalid																		
'11F5'	Token data hash result invalid																		
'11F6'	Length of ICC Public Key Modulus does not match Signed Dynamic Application Data																		
'12xx' – '13xx'	Declined																		
'1200'	No further details																		
'1201'	Restricted card																		
'1202'	Cancellation cannot be accepted (National use)																		
'1203'	National use																		
'1204'	Unknown Action Code																		
'1205'	Service is not allowed																		
'1206'	Service Code; card not for international use																		
'1207'	Card on Stop List																		
'1208'	PI-Card Type not legal for this transaction request																		
'1209'	Forced CVM not allowed																		
'120A'	CVM not allowed																		

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
'120B'	Transaction declined by host																		
'120C'	Unable to locate previous message (National use)																		
'120D'	Data are inconsistent with original data (National use)																		
'120E'	Transaction declined by ICC																		
'120F'	Voice authorization rejected																		
'1210'	Cryptogram format error																		
'1211'	Declined by Terminal/PSAM (TAC-Denial)																		
'1212'	Declined by Terminal/PSAM (IAC-Denial)																		
'1213'	Declined by Terminal/PSAM (TAC-Default)																		
'1214'	Declined by Terminal/PSAM (IAC-Default)																		
'1215'	Declined by Terminal/PSAM																		
'1216'	Only goods and services are allowed for this card																		
'1217'	Balance Inquiry Amount not available																		
'1218'	Accumulated Amount – Ceiling exceeded																		
'1219'	Accumulated Amount – Offline Ceiling exceeded																		
'1220'	PIN data required																		
'1221'	Incorrect PIN																		
'1222'	Service Code; ICC to be used																		
'1223'	Key Entered transaction is not allowed																		
'1224'	Fallback is not allowed																		
'1225'	Service not allowed																		
'1226'	CDA failed																		
'1230'	Card entry found, but below low-range (National use)																		
'1231'	PAN length not according to table-entr. (National use)																		
'1232'	Card not effective																		
'1233'	Incorrect PAN length																		
'1234'	Luhn check digit incorrect																		
'1235'	Dankort check digit incorrect																		
'1236'	PAN mismatch																		
'1237'	Track2 Equivalent Data length error																		
'1240'	Expired card																		
'1250'	Invalid amount																		
'1260'	Exceeds withdrawal amount limit																		
'1261'	Amount exceeds ceiling																		
'1262'	Amount exceeds offline ceiling																		
'1270'	Suspected fraud																		
'1271'	Suspected counterfeit card																		
'1275'	Amount not confirmed/accepted																		
'1276'	Transaction interrupted																		
'1277'	Extended Authorization terminated																		
'1280'	Invalid PIN block																		

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S	S	M	F	C	E	I	A	D	P	S	C	V	G	S	G	
			t	u	S	i	o	x	n	d	e	S	r	a	a	e	e	e	
			a	p															
'1281'	PIN length error																		
'1282'	PIN key synchronization error																		
'1283'	Terminal Action Code (TAC) could not be selected																		
'1290'	Exceeds withdrawal frequency limit																		
'12A0'	Forced offline not allowed																		
'12A1'	Online transactions not allowed for this Terminal Type																		
'12A2'	Offline transactions not allowed for this Terminal Type																		
'12A3'	Invalid Terminal Type																		
'12A4'	Cashback service not available from issuer																		
'12A5'	Illegal DCC transaction																		
'12B0'	Card acceptor contact acquirer																		
'12B1'	Card acceptor call acquirer's security department																		
'12B2'	Refer to issuer																		
'12B3'	Refer to issuer's special conditions																		
'12B4'	Unacceptable fee																		
'12B5'	No account of type requested																		
'12B6'	Requested function not supported																		
'12B7'	Not sufficient funds																		
'12B8'	Security violation																		
'12B9'	Invalid date (National use)																		
'12BA'	Honour with identification																		
'12BB'	Approved for partial amount																		
'12C0'	Allowable PIN tries exceeded																		
'12D0'	Invalid merchant																		
'12E0'	Invalid card number																		
'12E1'	No card record																		
'12E2'	Unknown card																		
'12E3'	AID not supported																		
'12E4'	AID error																		
'12E5'	Token requires terminal supporting signature																		
'12F0'	Loyalty card accepted																		
'1300'	Match on previous transaction																		
'1310'	Transaction not permitted to cardholder																		
'1311'	Transaction not permitted to terminal																		
'1312'	Violation of law																		
'1313'	Supplementary Authorization not allowed																		
'1314'	Cancellation can not be performed (No image)																		
'1315'	Cancellation can not be performed (Time-out)																		

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
	'1316'	Cancellation can not be performed (File in Data Store not to be found)																	
	'1317'	Cancellation can not be performed (Advice could not be deleted)																	
	'1320'	External authentication error																	
	'1321'	No Selectable Kernel Configurations Data																	
	'1322'	Online transaction required for Cashback																	
	'1323'	Transaction Identifier not identical to the one presented previously																	
'14xx'	Declined – Try Again with other Parameters																		
	'1400'	Select other application																	
	'1410'	Currency not supported																	
	'1420'	Card not present																	
'15xx'	Declined – Pick up																		
	'1500'	No further details																	
	'1501'	Expired card																	
	'1502'	Suspected fraud																	
	'1503'	Card acceptor contact acquirer																	
	'1504'	Restricted card																	
	'1505'	Card acceptor call acquirer's security department																	
	'1506'	Allowable PIN tries exceeded																	
	'1507'	Special conditions																	
	'1508'	Lost card																	
	'1509'	Stolen card																	
	'150A'	Suspected counterfeit card																	
	'150B'	Card on Stop List, pick-up requested																	
'16xx'	Failed – Retry																		
	'1600'	Condition of use not satisfied																	
	'1601'	Re-enter transaction																	
	'1602'	Format error																	
	'1603'	Cutover in progress																	
	'1604'	Card issuer or switch inoperative																	
	'1605'	Transaction destination cannot be found for routing																	
	'1606'	System malfunction																	
	'1607'	Card issuer signed off																	
	'1608'	Card issuer timed out																	
	'1609'	Card issuer unavailable																	
	'160A'	Not able to trace back to original transaction																	
	'160B'	Reconciliation cutover or checkpoint error																	
	'160C'	MAC incorrect																	
	'160D'	MAC key synchronization error																	
	'160E'	No communication keys available for use																	

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
'17xx'			Failed – No Retry																
	'1700'	Card error – No information given																	
	'1701'	Data not found																	
	'1702'	Previous transaction was not successful		☐															
	'1703'	Transaction declined by merchant/cardholder/terminal																	
	'1704'	Signature rejected																	
	'1705'	Goods or services not delivered																	
	'1706'	Invalid transaction status																	
	'1707'	Second Complete Payment rejected by PSAM																	
	'171E'	Service Code; format error																	
	'1760'	Data not found																	
	'1761'	Data Store error – No information given																	
	'176D'	Transaction request illegal																	
	'176E'	LEN _{TRACK2} error																	
	'1770'	Acquirer not supported by switch														☐			
	'1780'	Invalid transaction														☐			
	'1781'	Checksum error – blocked temporary																	
	'1782'	Checksum error – blocked irreversibly																	
	'1783'	PSAM set to non-operational after patch update											☐						
	'1784'	KEY _{CDP} not present																	
	'1785'	KEY _{CDP} not loaded after Start-up PSAM																	
	'1786'	Decryption error																	
	'1787'	KEK _{CDP} not present																	
	'1788'	Undefined Key Type																	
	'17A0'	Duplicate transaction														☐			
	'17A1'	Message number out of sequence														☐			
	'17A2'	Violation of business arrangement														☐			
'1Axx'			RC Related (Card Handler)																
	'1A21'	Output buffer overflow																	
	'1A23'	Card did not respond																	
	'1A24'	No card in reader																	
	'1A25'	Unrecoverable Transmission Error																	
	'1A26'	Card buffer overflow																	
	'1A27'	Unrecoverable Protocol error																	
	'1A28'	Response has no status words																	
	'1A29'	Invalid buffer																	
	'1A2A'	Other card error																	
	'1A2B'	Card partially in reader																	
	'1AF2'	Time-out																	
	'1AF3'	Handler error																	
	'1AF4'	Handler must be initialized																	

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (continued)

ASW1-ASW2	Meaning	Commands	S t a r t U p	S u p p o r t A l d s	M S C T a b l e	F i l e C h a r a c t e r	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
	'1AF5'	Handler busy																	
	'1AF6'	Insufficient resources																	
	'1AF7'	Handler must be opened																	
	'1AFB'	Unsupported operation																	
'1Bxx' RC Related (User Interface Handler)																			
	'1B34'	Unknown Message Code																	
	'1B35'	Code Table not supported																	
	'1B80'	No KCV available, KSES not present																	
	'1B81'	Wrong PIN Pad ID																	
	'1B82'	Authentication Error (MAC Validation failed)																	
	'1B83'	PSAM Identifier not recognized																	
	'1B84'	Parameters out of range																	
	'1B85'	Key check values not identical, synchronization necessary																	
	'1B86'	PIN not available																	
	'1B87'	Secure Device not in PIN Entry State																	
	'1B88'	Termination failed																	
	'1B89'	Record not found																	
	'1B8A'	Signature error																	
	'1B8B'	Hash error																	
	'1B8C'	PSAM Certificate Error																	
	'1B8D'	Hash algorithm not supported																	
	'1B8E'	PSAM PK algorithm not supported																	
	'1B8F'	Hash result invalid																	
	'1B90'	RSA key mismatch. VKP _{CA} , PSAM not recognized																	
	'1BF2'	Time-out																	
	'1BF3'	Handler error																	
	'1BF4'	Handler must be initialized																	
	'1BF5'	Handler busy																	
	'1BF6'	Insufficient resources																	
	'1BF7'	Handler must be opened																	
	'1BFB'	Unsupported operation																	
'1Cxx' RC Related (Merchant Application Handler)																			
	'1C40'	Invalid Currency																	
	'1C41'	Invalid Currency Exponent																	
	'1CF2'	Time-out																	
	'1CF3'	Handler error																	
	'1CF4'	Handler must be initialized																	
	'1CF5'	Handler busy																	
	'1CF6'	Insufficient resources																	

Table 2-14.157 - Debit/Credit PSAM generated ASW1-ASW2s (1) (concluded)

ASW1-ASW2	Meaning	Commands	S t a r t U P	S u p p A I D s	M S C T a b l e	F i l e C h a r a c	C o n f i g u r e	E x c h a n g e	I n s t a l l	A d d e n d u m	D e a c t i v a t e	P S A M U p d a t e	S y n c h r o n i z e	C r e a t e S R	V a l i d - a t e I n	G e t D / C P r o p	S e t D / C P r o p	G e t P C T	
	'1CF7'	Handler must be opened	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1CFB'	Unsupported operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
'1Dxx'	RC Related (Data Store Handler)																		
	'1D51'	Invalid File ID																	
	'1D52'	Record too large																	
	'1D53'	Search key too large																	
	'1D55'	File could not be accessed																	
	'1D57'	File read error																	
	'1D58'	File write error																	
	'1D59'	Search key already existing																	
	'1DF2'	Time-out	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1DF3'	Handler error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1DF4'	Handler must be initialized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1DF5'	Handler busy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1DF6'	Insufficient resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1DF7'	Handler must be opened	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
	'1DFB'	Unsupported operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
'61xx' – '6Fxx'	Card errors conveyed transparently																		
	'61L _a '	SW2 indicates the number of response bytes still available																	
	'6300'	State of non-volatile memory unchanged; authentication failed																	
	'63Cx'	State of non-volatile memory unchanged; counter provided by 'x' (from 0–15)																	
	'6983'	Command not allowed; authentication method blocked																	
	'6984'	Command not allowed; referenced data invalidated																	
	'6985'	Command not allowed; condition of use not satisfied																	
	'6A81'	Wrong parameter(s) P1 P2; function not supported																	
	'6A83'	Wrong parameter(s) P1 P2; record not found																	
	'6A88'	Referenced data (data objects) not found																	
'91xx' – '9Fxx'	Card errors conveyed transparently																		

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K
'00xx'	Successful (TAPA defined)																
'0000'	Successful	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'02xx'	(TAPA defined)																
'0200'	No information given	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'0201'	Application not supported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'0202'	Function not supported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'0203'	PIN Pad is unresponsive	<input type="checkbox"/>	<input type="checkbox"/>														
'0204'	PIN Pad unable to synchronize	<input type="checkbox"/>	<input type="checkbox"/>														
'10xx'	Approved/Successful – Action Requested																
'1000'	Configuration required																
'1001'	Installation required																
'1002'	Restart required																
'1003'	New data available																
'1010'	Approved (VIP)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1011'	Approved, update ICC									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1012'	Approved (National use)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1013'	Approved (National use)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1014'	Approved (National use)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1015'	Approved (National use)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1016'	Approved (National use)									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1020'	No issuer response									<input type="checkbox"/>							
'1021'	Processing Condition Table (PCT) inconsistent																
'1022'	Extended Authorization interrupted	<input type="checkbox"/>															
'1023'	KEY _{CDP} not present	<input type="checkbox"/>															
'1030'	No CVM performed successfully	<input type="checkbox"/>															
'1031'	Offline PIN validation failed	<input type="checkbox"/>															
'1032'	PAN mismatch	<input type="checkbox"/>															
'1033'	Requested transaction not found																
'1034'	Format error in host message, offline approved									<input type="checkbox"/>							
'1035'	Amount exceeds offline ceiling					<input type="checkbox"/>											
'1036'	Amount exceeds ceiling					<input type="checkbox"/>											
'1037'	Expiry Check not performed by terminal		<input type="checkbox"/>														
'1038'	Service Code not interpreted		<input type="checkbox"/>														
'1039'	Checksum error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
'103A'	Checksum error – Service Record generated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
'103F'	Statistics data removed due to maximum envelope data					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								
'1040'	Envelope data exceeds the capability of the PSAM version																
'1041'	Delivery of data for the envelope is too late																
'1042'	Format error while sending data in the envelope																
'1043'	Service Pack not supported by PSAM																
'1044'	Merchant Application Log failed													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1057'	AIP does not indicate DDA					<input type="checkbox"/>											

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K
'1058'	Mandatory data is missing	☐															
'1059'	Redundant data objects (command)	☐															
'105A'	Thread unknown (soft)												☐	☐	☐	☐	
'105F'	Length of modulus does not match Issuer Certificate	☐															
'1060'	Issuer Certificate format error	☐															
'1061'	Issuer Certificate invalid	☐															
'1062'	Issuer Identification Number mismatch	☐															
'1063'	Card Certificate format error	☐															
'1064'	ICC Certificate PAN mismatch	☐															
'1065'	DDOL Tag error	☐															
'1066'	Length of modulus does not match Card Certificate	☐															
'1067'	DAD format error	☐															
'1068'	ICC PIN Certificate PAN mismatch	☐															
'1069'	Missing Signed Dynamic Application Data	☐															
'106A'	Length of modulus does not match SDA data	☐															
'106B'	SDA/DDA source error	☐															
'106C'	SDA tag error	☐															
'106D'	SDA format error	☐															
'106E'	AID length error	☐															
'106F'	Length of ICC Public Key Modulus does not match Signed Dynamic Application Data	☐															
'1070'	Issuer Certificate expired	☐															
'1071'	Card Certificate expired	☐															
'1072'	Key mismatch	☐															
'1073'	Issuer Certificate algorithm not supported	☐															
'1074'	Issuer Certificate hash algorithm not supported	☐															
'1075'	Issuer Certificate hash result invalid	☐															
'1076'	Card Certificate hash algorithm not supported	☐															
'1077'	Card Certificate algorithm not supported	☐															
'1078'	Card Certificate hash result invalid	☐															
'1079'	DAD hash algorithm not supported	☐															
'107A'	DAD hash result invalid	☐															
'107B'	SDA hash algorithm not supported	☐															
'107C'	SDA hash result invalid	☐															
'107D'	Length of modulus does not match ICC PIN Certificate	☐															
'107E'	ICC PIN Certificate format error	☐															
'107F'	ICC PIN Certificate expired	☐															
'1080'	ICC PIN Certificate invalid	☐															
'1081'	ICC PIN Certificate hash algorithm not supported	☐															
'1082'	ICC PIN Certificate algorithm not supported	☐															
'1083'	ICC PIN Certificate hash result invalid	☐															
'1084'	PIN try counter not readable	☐															
'1087'	Script command syntax error									☐							

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K
'1088'	TLV error in proprietary record	☐															
'1089'	Script Tag error	☐							☐								
'1090'	Unpredictable Number missing in CDOL								☐								
'1091'	Cryptogram Information Data mismatch					☐											
'1092'	Hash (Signature) wrong					☐											
'1093'	Hash (Transaction Data) wrong					☐											
'1094'	Header/Trailer format error					☐											
'1095'	Expired card																
'10AB'	PTS activated																
'10B2'	Refer to card issuer	☐															
'10B3'	Refer to card issuer's special conditions	☐															
'10CA'	Data not available																
'10CB'	PIN Pad PK record not found	☐															
'10CC'	PSAM Certificate error	☐															
'10CD'	Hash algorithm not supported	☐															
'10CE'	PSAM PK algorithm not supported	☐															
'10CF'	Hash result invalid	☐															
'10D0'	RSA key mismatch	☐															
'10D1'	PSAM identifier not recognized	☐															
'10D2'	Signature error	☐															
'10D3'	PPC Certificate format error	☐															
'10D4'	PPC Certificate ID mismatch	☐															
'10D5'	PPC Certificate expired	☐															
'10D6'	PPC Certificate hash algorithm not supported	☐															
'10D7'	PPC Certificate algorithm not supported	☐															
'10D8'	PPC Certificate hash result invalid	☐															
'10D9'	PP Certificate format error	☐															
'10DA'	PP Certificate hash algorithm not supported	☐															
'10DB'	PP Certificate ID mismatch	☐															
'10DC'	PP Certificate expired	☐															
'10DD'	PP Certificate algorithm not supported	☐															
'10DE'	PP Certificate hash result invalid	☐															
'10DF'	PP Certificate Creator ID mismatch	☐															
'10E0'	PIN Pad table full	☐															
'10E1'	Wrong LPKM in certificate record	☐															
'10E2'	Wrong record tag in certificate record	☐															
'10E3'	Wrong data length in certificate record	☐															
'10E4'	PIN Pad not synchronized	☐															
'10E5'	Tag error 1	☐															
'10E6'	Tag error 2	☐															
'10E7'	Tag length error 1	☐															
'10E8'	Tag length error 2	☐															

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
	'10E9'	ICC and Terminal have different Application Versions	<input type="checkbox"/>															
	'10EA'	Requested Service not allowed for card product	<input type="checkbox"/>															
	'10EB'	Application not yet effective	<input type="checkbox"/>															
	'10EC'	Expired Application	<input type="checkbox"/>															
	'10ED'	Identifier not supported																
	'10EE'	Wrong AID length																
	'10EF'	AID not found in AID Table																
	'10F0'	PAN not found in MSC Table																
	'10F1'	Syntax error (input data)																
	'10F2'	Local PIN disabled																
	'10F3'	Luhn check digit incorrect																
	'10F4'	PAN-length not according to table-entry	<input type="checkbox"/>	<input type="checkbox"/>														
	'10F5'	Identifier not allowed for this transaction	<input type="checkbox"/>	<input type="checkbox"/>														
	'10F6'	Unknown Track3	<input type="checkbox"/>	<input type="checkbox"/>														
	'10F7'	Extended Issuer Envelope not supported according to Terminal Settings																
	'10FB'	Fallback allowed												<input type="checkbox"/>				
	'10FF'	Incorrect PIN, next CVM selected	<input type="checkbox"/>															
'11xx'	Error – Action Requested																	
	'1100'	Start-up PSAM command required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1101'	Restart required																
	'1110'	Outstanding transaction must be completed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1111'	Command out of sequence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1120'	Data incorrect	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1121'	State error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1122'	INS not supported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1123'	Chain error																
	'1124'	KCV error																
	'1125'	Segment no. error								<input type="checkbox"/>								
	'1126'	Too many segments																
	'1127'	PKx too long																
	'1128'	Wrong length for this Tag																
	'1129'	Hash error																
	'112A'	Parity error																
	'112B'	Tag out of range																
	'112C'	Syntax error in date	<input type="checkbox"/>															
	'112D'	Segment too long																
	'112E'	Tag changed between segments																
	'112F'	L _c error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1130'	LEN _{APDU} error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1131'	MAC error in command																
	'1132'	MDOL2 data present																
	'1133'	MDOL1 data missing					<input type="checkbox"/>	<input type="checkbox"/>										
	'1134'	MDOL2 data missing								<input type="checkbox"/>	<input type="checkbox"/>							

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
'1135'	Counter number out of range																	
'1136'	CKTOKEN Key is missing	☐	☐	☐	☐													
'1137'	LENMDOL error					☐	☐			☐	☐							
'1138'	Cryptogram Information Data (plaintext & signed) mismatch					☐	☐	☐	☐									
'1139'	Hash (Signature) wrong					☐												
'113A'	Hash (Transaction Data) wrong					☐												
'113B'	Header/Trailer format error					☐												
'1140'	Data Store Handler must be opened														☐	☐	☐	☐
'1141'	Data Store full														☐	☐	☐	☐
'1142'	Duplicate File IDs																	
'1143'	Invalid File ID														☐	☐	☐	☐
'1144'	Total Issuer Envelope Data exceeds buffer size					☐	☐	☐										
'1145'	Extended Issuer Envelope not supported according to Terminal Settings					☐	☐	☐										
'1150'	PSAM deactivated	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
'1151'	PSAM Busy – Try later	☐	☐	☐	☐													
'1152'	Deactivation rejected																	
'1153'	PSAM disabled	☐	☐	☐	☐	☐												
'1154'	Illegal PSAM Life Cycle	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
'1155'	Entry number out of range									☐	☐	☐	☐					
'1156'	PSAM not operational																	
'1157'	Date older																	
'1158'	Thread unknown					☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
'1159'	Memory failure	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
'115A'	PSAM busy – Active threads																	
'115B'	Version obsolete																	
'115C'	Record length error																	
'115D'	CVM List formatting error	☐																
'115F'	PTS Tag 9B error	☐																
'1160'	Tag format error	☐																
'1161'	Missing AIP	☐																
'1162'	Missing AFL	☐																
'1163'	Length of AFL is not multiple of four	☐																
'1164'	AFL byte error	☐																
'1165'	Tag 70 is missing	☐																
'1166'	Tag 70 length error	☐																
'1167'	SFI range error	☐																
'1168'	Redundant data objects	☐																
'1169'	Mandatory data is missing 2	☐																
'116A'	Tag error 1	☐																
'116B'	Tag error 2	☐																
'116C'	Tag length error 1	☐																
'116D'	Tag length error 2	☐																

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K
'116E'	FCI data missing	☐															
'116F'	DOL data out of range	☐															
'1170'	Account Type format error																
'1171'	Timestamp is old																
'1172'	FWVersion _{BASE} not found																
'1173'	RunVersion _{TARGET} not found																
'1174'	FWVersion _{BASE} changed																
'1175'	RunVersion _{TARGET} changed																
'1176'	Operational Status changed																
'1177'	TOTAL _{BODY} out of range																
'1178'	Not possible to switch to any operational version																
'1179'	Body no. out of range																
'117A'	Addresses out of range																
'1180'	Mismatch between POS Entry Mode and Card Data Source	☐	☐	☐	☐												
'1181'	Unknown Data Request			☐	☐												
'1182'	Card Data Source error	☐	☐	☐	☐												
'1183'	Card Handler error – No information given	☐	☐			☐	☐			☐	☐						
'1184'	Card Reader must be opened	☐	☐														
'1185'	Token not expected	☐	☐	☐													
'1186'	Token missing				☐												
'1187'	Amount missing	☐	☐	☐	☐												
'1188'	Unknown Transaction Type	☐	☐	☐	☐												
'1189'	Track2 missing		☐														
'118A'	Invalid MI request	☐	☐	☐	☐					☐	☐						
'118B'	Authentication error (MAC validation failed)	☐	☐							☐	☐						
'118C'	LEN _{STAT} error	☐	☐	☐	☐												
'118D'	Amount format error	☐	☐	☐	☐												
'118E'	Invalid Token Format				☐												
'118F'	Invalid Token				☐												
'1190'	Incorrect padding for encipherment				☐												
'1191'	Mismatch between Token Info and Token Transaction Data				☐												
'1193'	Cash or cashback not supported by terminal	☐	☐	☐	☐												
'1194'	PSAM Cash functionality not enabled	☐	☐	☐	☐												
'1195'	Goods or Services not supported by the terminal	☐	☐	☐	☐												
'1196'	Option not supported																
'1197'	Illegal SW1-SW2 format	☐				☐				☐							
'11C0'	Wrong PIN Pad ID																
'11C1'	Key Check value not identical																
'11C2'	Secure Device not in PIN Entry State																
'11C3'	Termination failed																
'11C4'	Length of modulus does not match	☐															
'11C5'	ICC PIN certificate format error	☐															

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K
'11C6'	ICC PIN certificate expired	☐															
'11C7'	ICC PIN certificate invalid	☐															
'11C8'	ICC PIN certificate hash algorithm not supported	☐															
'11C9'	ICC PIN certificate algorithm not supported	☐															
'11CA'	ICC PIN certificate hash result invalid	☐															
'11CB'	PIN Pad PK record not found																
'11CC'	PSAM Certificate error																
'11CD'	Hash algorithm not supported																
'11CE'	PSAM PK algorithm not supported																
'11CF'	Hash result invalid																
'11D0'	RSA key mismatch																
'11D1'	PSAM identifier not recognized																
'11D2'	Signature error	☐	☐														
'11D3'	PPC Certificate format error																
'11D4'	PPC Certificate ID mismatch																
'11D5'	PPC Certificate expired																
'11D6'	PPC Certificate hash algorithm not supported																
'11D7'	PPC Certificate algorithm not supported																
'11D8'	PPC Certificate hash result invalid																
'11D9'	PP Certificate format error																
'11DA'	PP Certificate hash algorithm not supported																
'11DB'	PP Certificate ID mismatch																
'11DC'	PP Certificate expired																
'11DD'	PP Certificate algorithm not supported																
'11DE'	PP Certificate hash result invalid																
'11DF'	PP Certificate Creator ID mismatch																
'11E0'	PIN Pad table full																
'11E1'	Wrong LPKM in certificate record																
'11E2'	Wrong record tag in certificate record																
'11E3'	Wrong data length in certificate record																
'11E4'	PIN Pad not synchronized	☐	☐														
'11E5'	Unknown state	☐	☐														
'11E6'	State address not found	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
'11E7'	Command address not found	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
'11E8'	Key mismatch (Token)				☐												
'11E9'	Length of modulus does not match Token Certificate				☐												
'11EA'	Token Certificate format error				☐												
'11EB'	Token Certificate expired				☐												
'11EC'	Token Certificate hash algorithm not supported				☐												
'11ED'	Token Certificate algorithm not supported				☐												
'11EE'	Token Certificate hash result invalid				☐												
'11EF'	CDOL1 error				☐												

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
'11F0'	CDOL2 error									☐								
'11F1'	TDOL error					☐				☐								
'11F2'	Format error (Generate AC1 response)					☐												
'11F3'	Format error (Generate AC2 response)									☐								
'11F4'	Token length invalid																	
'11F5'	Token data hash result invalid					☐												
'11F6'	Length of ICC Public Key Modulus does not match Signed Dynamic Application Data					☐												
'12xx' – '13xx'	Declined																	
'1200'	No further details									☐	☐	☐	☐					
'1201'	Restricted card									☐	☐	☐	☐					
'1202'	Cancellation cannot be accepted (National use)									☐	☐	☐	☐					
'1203'	National use									☐	☐	☐	☐					
'1204'	Unknown Action Code									☐	☐	☐	☐					
'1205'	Service is not allowed	☐	☐		☐													
'1206'	Service Code; card not for international use																	
'1207'	Card on Stop List							☐	☐	☐								
'1208'	PI-Card Type not legal for this transaction request							☐	☐	☐								
'1209'	Forced CVM not allowed	☐	☐	☐	☐													
'120A'	CVM not allowed																	
'120B'	Transaction declined by host									☐	☐	☐	☐					
'120C'	Unable to locate previous message (National use)									☐	☐	☐	☐					
'120D'	Data are inconsistent with original data (National use)									☐	☐	☐	☐					
'120E'	Transaction declined by ICC							☐		☐								
'120F'	Voice authorization rejected							☐	☐	☐								
'1210'	Cryptogram format error							☐										
'1211'	Declined by Terminal/PSAM (TAC-Denial)							☐										
'1212'	Declined by Terminal/PSAM (IAC-Denial)							☐										
'1213'	Declined by Terminal/PSAM (TAC-Default)							☐										
'1214'	Declined by Terminal/PSAM (IAC-Default)							☐										
'1215'	Declined by Terminal/PSAM							☐										
'1216'	Only goods and services are allowed for this card							☐										
'1217'	Balance Inquiry Amount not available							☐										
'1218'	Accumulated Amount – Ceiling exceeded																☐	
'1219'	Accumulated Amount – Offline Ceiling exceeded																☐	
'1220'	PIN data required									☐	☐	☐	☐					
'1221'	Incorrect PIN									☐	☐	☐	☐					
'1222'	Service Code; ICC to be used		☐															
'1223'	Key Entered transaction is not allowed			☐														
'1224'	Fallback is not allowed	☐	☐	☐														
'1225'	Service not allowed							☐										
'1226'	CDA failed							☐		☐								
'1230'	Card entry found, but below low-range (National use)									☐	☐	☐	☐					
'1231'	PAN-length not according to table-ent. (National use)									☐	☐	☐	☐					

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K
'1232'	Card not effective																
'1233'	Incorrect PAN length																
'1234'	Luhn check digit incorrect																
'1235'	Dankort check digit incorrect																
'1236'	PAN mismatch																
'1237'	Track2 Equivalent Data length error																
'1240'	Expired card																
'1250'	Invalid amount																
'1260'	Exceeds withdrawal amount limit																
'1261'	Amount exceeds ceiling																
'1262'	Amount exceeds offline ceiling																
'1270'	Suspected fraud																
'1271'	Suspected counterfeit card																
'1275'	Amount not confirmed/accepted																
'1276'	Transaction interrupted																
'1277'	Extended Authorization terminated																
'1280'	Invalid PIN block																
'1281'	PIN length error																
'1282'	PIN key synchronization error																
'1283'	Terminal Action Code (TAC) could not be selected																
'1290'	Exceeds withdrawal frequency limit																
'12A0'	Forced offline not allowed																
'12A1'	Online transactions not allowed for this Terminal Type																
'12A2'	Offline transactions not allowed for this Terminal Type																
'12A3'	Invalid Terminal Type																
'12A4'	Cashback service not available from issuer																
'12A5'	Illegal DCC transaction																
'12B0'	Card acceptor contact acquirer																
'12B1'	Card acceptor call acquirer's security department																
'12B2'	Refer to issuer																
'12B3'	Refer to issuer's special conditions																
'12B4'	Unacceptable fee																
'12B5'	No account of type requested																
'12B6'	Requested function not supported																
'12B7'	Not sufficient funds																
'12B8'	Security violation																
'12B9'	Invalid date (National use)																
'12BA'	Honour with identification																
'12BB'	Approved for partial amount																
'12C0'	Allowable PIN tries exceeded																
'12D0'	Invalid merchant																
'12E0'	Invalid card number																

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
'12E1'	No card record																	
'12E2'	Unknown card																	
'12E3'	AID not supported																	
'12E4'	AID error																	
'12E5'	Token requires terminal supporting signature																	
'12F0'	Loyalty card accepted																	
'1300'	Match on previous transaction																	
'1310'	Transaction not permitted to cardholder																	
'1311'	Transaction not permitted to terminal																	
'1312'	Violation of law																	
'1313'	Supplementary Authorization not allowed																	
'1314'	Cancellation can not be performed (No image)																	
'1315'	Cancellation can not be performed (Time-out)																	
'1316'	Cancellation can not be performed (File in Data Store not to be found)																	
'1317'	Cancellation can not be performed (Advice could not be deleted)																	
'1320'	External authentication error																	
'1321'	No Selectable Kernel Configurations Data																	
'1322'	Online transaction required for Cashback																	
'1323'	Transaction Identifier not identical to the one presented previously																	
'14xx'	Declined – Try Again with other Parameters																	
'1400'	Select other application																	
'1410'	Currency not supported																	
'1420'	Card not present																	
'15xx'	Declined – Pick up																	
'1500'	No further details																	
'1501'	Expired card																	
'1502'	Suspected fraud																	
'1503'	Card acceptor contact acquirer																	
'1504'	Restricted card																	
'1505'	Card acceptor call acquirer's security department																	
'1506'	Allowable PIN tries exceeded																	
'1507'	Special conditions																	
'1508'	Lost card																	
'1509'	Stolen card																	
'150A'	Suspected counterfeit card																	
'150B'	Card on Stop List, pick-up requested																	
'16xx'	Failed – Retry																	
'1600'	Condition of use not satisfied																	
'1601'	Re-enter transaction																	
'1602'	Format error																	

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
'1603'	Cutover in progress																	
'1604'	Card issuer or switch inoperative																	
'1605'	Transaction destination cannot be found for routing																	
'1606'	System malfunction																	
'1607'	Card issuer signed off																	
'1608'	Card issuer time out																	
'1609'	Card issuer unavailable																	
'160A'	Not able to trace back to original transaction																	
'160B'	Reconciliation cutover or checkpoint error																	
'160C'	MAC incorrect																	
'160D'	MAC key synchronization error																	
'160E'	No communication keys available for use																	
'160F'	Encryption key synchronization error																	
'1610'	Key Entered data out of range																	
'1611'	Security software/hardware error – try again																	
'1612'	Security software/hardware error – no action																	
'1613'	Request in progress																	
'1614'	Host time-out (Private use)																	
'1615'	No valid conversion for a field value (National use)																	
'1616'	PIN not available																	
'1617'	Time-out																	
'1618'	No Host Data received																	
'1619'	Invalid Terminal Identification																	
'1630'	Invalid data received																	
'1631'	MTI error																	
'1632'	Bit map error																	
'1633'	STAN mismatch																	
'1634'	Time mismatch																	
'1635'	Date mismatch																	
'1636'	GMT offset mismatch																	
'1637'	Card Accepting Device mismatch																	
'1638'	PSAM Identifier error																	
'1639'	MAC validation failed																	
'163A'	MAD-Handler ID mismatch																	
'163B'	Terminal Approval No. mismatch																	
'1640'	No response from card																	
'1641'	Track2 format error																	
'1642'	Track3 format error																	
'1650'	All entries in use – New thread cannot be started																	
'1651'	Fatal error																	
'1652'	Fatal command error																	

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
'17xx'		Failed – No Retry																
	'1700'	Card error – No information given	<input type="checkbox"/>				<input type="checkbox"/>				<input type="checkbox"/>							
	'1701'	Data not found																
	'1702'	Previous transaction was not successful																
	'1703'	Transaction declined by merchant/cardholder/terminal													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1704'	Signature rejected													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1705'	Goods or services not delivered													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1706'	Invalid Transaction Status													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1707'	Second Complete Payment rejected by PSAM													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'171E'	Service Code; format error																
	'1760'	Data not found	<input type="checkbox"/>				<input type="checkbox"/>				<input type="checkbox"/>							
	'1761'	Data Store error – No information given													<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'176D'	Transaction request illegal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'176E'	LENT _{TRACK2} error		<input type="checkbox"/>														
	'1770'	Acquirer not supported by switch									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	'1780'	Invalid transaction									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	'1781'	Checksum error – blocked temporary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1782'	Checksum error – blocked irreversibly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1783'	PSAM set to non--operational after patch update	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1784'	KEY _{CDP} not present	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1785'	KEY _{CDP} not loaded after Start-up PSAM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1786'	Decryption error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1787'	KEK _{CDP} not present	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1788'	Undefined Key Type	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'17A0'	Duplicate transaction									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	'17A1'	Message number out of sequence									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	'17A2'	Violation of business arrangement									<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
'1Axx'		RC Related (Card Handler)																
	'1A21'	Output buffer overflow		<input type="checkbox"/>														
	'1A23'	Card did not respond	<input type="checkbox"/>															
	'1A24'	No card in reader	<input type="checkbox"/>															
	'1A25'	Unrecoverable Transmission Error	<input type="checkbox"/>															
	'1A26'	Card buffer overflow	<input type="checkbox"/>															
	'1A27'	Unrecoverable Protocol error	<input type="checkbox"/>															
	'1A28'	Response has no status words	<input type="checkbox"/>															
	'1A29'	Invalid buffer	<input type="checkbox"/>															
	'1A2A'	Other card error	<input type="checkbox"/>															
	'1A2B'	Card partially in reader	<input type="checkbox"/>															
	'1AF2'	Time-out	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1AF3'	Handler error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1AF4'	Handler must be initialized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1AF5'	Handler busy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 2-14.158 - Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete				
		E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	E M V	M S C	K E Y	T O K	
	'1AF6'	Insufficient resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1AF7'	Handler must be opened	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1AFB'	Unsupported operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1Bxx'	RC Related (User Interface Handler)																	
	'1B34'	Unknown Message Code	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1B35'	Code Table not supported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>												
	'1B80'	No KCV available, KSES not present	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B81'	Wrong PIN Pad ID	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B82'	Authentication Error (MAC Validation failed)	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B83'	PSAM Identifier not recognized	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B84'	Parameters out of range	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B85'	Key check values not identical, synchronization necessary	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B86'	PIN not available	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B87'	Secure Device not in PIN Entry State	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B88'	Termination failed	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B89'	Record not found	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B8A'	Signature error	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B8B'	Hash error	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B8C'	PSAM Certificate Error	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B8D'	Hash algorithm not supported	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B8E'	PSAM PK algorithm not supported	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B8F'	Hash result invalid	<input type="checkbox"/>	<input type="checkbox"/>														
	'1B90'	RSA key mismatch. VKP _{CA, PSAM} not recognized	<input type="checkbox"/>	<input type="checkbox"/>														
	'1BF2'	Time-out	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1BF3'	Handler error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1BF4'	Handler must be initialized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1BF5'	Handler busy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1BF6'	Insufficient resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1BF7'	Handler must be opened	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1BFB'	Unsupported operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
'1Cxx'	RC Related (Merchant Application Handler)																	
	'1C40'	Invalid Currency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>													
	'1C41'	Invalid Currency Exponent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>													
	'1CF2'	Time-out	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1CF3'	Handler error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1CF4'	Handler must be initialized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1CF5'	Handler busy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1CF6'	Insufficient resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1CF7'	Handler must be opened	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	'1CFB'	Unsupported operation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2-14.10.2 ASW1-ASW2 Applicable for Local PIN

Table 2-14.159 - Approved/Successful

ASW1-ASW2	APACS	Meaning	Description
'0000'	-	Successful	No further action.

Table 2-14.160 - Approved/Successful - Action Requested

ASW1-ASW2	APACS	Meaning	Description
'10F2'	-	Local PIN disabled	Get Debit/Credit Properties

Table 2-14.161 - Error - Action Requested

ASW1-ASW2	APACS	Meaning	Description
'1F00'	-	Local PIN disabled	The Local PIN Validation functionality is disabled
'1F01'	-	Method Number has illegal value	Related to the <i>Local PIN Validation</i> command
'1F02'	-	Min. PIN digits illegal	Related to the <i>Local PIN Validation</i> command
'1F03'	-	Max. PIN digits illegal	Related to the <i>Local PIN Validation</i> command
'1F04'	-	Min. PIN digits greater than max. PIN digits	Related to the <i>Local PIN Validation</i> command
'1F05'	-	Number of PIN tries left has illegal value	Related to the <i>Local PIN Validation</i> command
'1F06'	-	Last PIN incorrect has illegal value	Related to the <i>Local PIN Validation</i> command
'1F07'	-	Timer Flag has illegal value	Related to the <i>Local PIN Validation</i> command
'1F08'	-	LEN _{AMOUNT} has illegal value	Related to the <i>Local PIN Validation</i> command
'1F09'	-	LEN _{MSCD} has illegal value (Method Number '00')	Related to the <i>Local PIN Validation</i> command
'1F0A'	-	LEN _{MSCD} has illegal value (Method Number '01')	Related to the <i>Local PIN Validation</i> command
'1F0B'	-	PIN Pad not synchronized	Related to the <i>Local PIN Validation</i> command
'1F0C'	-	Wrong control field in MSCD plaintext PIN block	Related to the <i>Local PIN Validation</i> command
'1F0D'	-	PIN length (N) from MSCD plaintext PIN block different	Related to the <i>Local PIN Validation</i> command
'1F0E'	-	MSCD plaintext PIN block filler error	Related to the <i>Local PIN Validation</i> command
'1F10'	-	Key chain not loaded in PSAM	Related to the <i>Local PIN Validation</i> command
'1F11'	-	Key version from MSCD different	Related to the <i>Local PIN Validation</i> command
'1F12'	-	Wrong padding in MSCD deciphered PIN data	Related to the <i>Local PIN Validation</i> command
'1F13'	-	Wrong control field in MSCD deciphered PIN block	Related to the <i>Local PIN Validation</i> command
'1F14'	-	PIN length (N) from MSCD deciphered PIN block different	Related to the <i>Local PIN Validation</i> command
'1F15'	-	MSCD deciphered PIN block filler error	Related to the <i>Local PIN Validation</i> command
'1F17'	-	Transaction Counter replay or no more PIN tries left	Related to the <i>Local PIN Validation</i> command
'1F18'	-	L _c max. limit exceeded	Related to the <i>Local PIN Validation</i> command
'1F19'	-	Transaction Counter offset exceeded	Related to the <i>Local PIN Validation</i> command
'1F1A'	-	Key chain has illegal value	Related to the <i>Local PIN Validation</i> command
'1F20'	-	Load method has illegal value	Related to the <i>Load LP Keys</i> command

Table 2-14.161 - Error - Action Requested (*concluded*)

ASW1-ASW2	APACS	Meaning	Description
'1F21'	–	Load LEN _{MSCD} illegal	Related to the <i>Load LP Keys</i> command
'1F22'	–	Load Key Chain illegal	Related to the <i>Load LP Keys</i> command
'1F23'	–	Unknown Key Type	Related to the <i>Load LP Keys</i> command
'1F24'	–	Load KEK KCV error	Related to the <i>Load LP Keys</i> command
'1F25'	–	Load Key KCV error	Related to the <i>Load LP Keys</i> command
'1F26'	–	Load KEK for selected key-chain not loaded	Related to the <i>Load LP Keys</i> command

Table 2-14.162 - Declined

ASW1-ASW2	APACS	Meaning	Description
'1F0F'	–	PIN from plaintext PIN block different	The plaintext PIN presented is declined. Related to the <i>Local PIN Validation</i> command
'1F16'	–	PIN from deciphered PIN block different	The enciphered PIN presented is declined. Related to the <i>Local PIN Validation</i> command

NOTE: In addition to the ASW1-ASW2 listed above, ASW1-ASW2 related to synchronization and length checks can be returned. Explanation of these values can be found in section 2-14.10.1 page 2-14-131.

This page is intentionally left blank

2-15 Data Elements

2-15.1 Introduction

In this section is a detailed overview of the formats of the individual fields in the commands, responses and data structures described in the previous sections.

For each data element, the following descriptors may be present:

- Reference (if present, it refers to an existing standard defining a similar data element).
- Purpose (a short description of the use for the given data element).
- Format (gives the size and type of the data element and possibly a symbolic format used to describe the contents).
- Contents (the exact definition for the coding of the data element).
- Remarks (other information).

2-15.1.1 Coding of Data Elements

- | | | |
|------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2-15.1.1.1 | A | All data elements sent and/or received on the interface between the CAD and PSAM and the interface between the CAD and Terminal Operator shall be coded according to the definitions in this chapter. |
| 2-15.1.1.2 | A | When a field of more than one byte has to be transmitted, the <i>most</i> significant byte shall be sent first. |

2-15.1.2 Data Elements Defined in EMV and TAPA

Data elements not listed in this chapter can be found in either ref. 20: "EMV ICC Specification" or in ref. 27: "TAPA, Application Architecture Specification".

2-15.2 Data Elements for the Debit/Credit Application

2-15.2.1 Account Type

Reference: Ref. 20: "Specification Update Bulletin No. 39: Definition of the new data element: Account Type".

Purpose: Indicates the type of account selected on the terminal.

Format: n2 (1 byte).

Contents: See table 2-15.1.

Remarks: Tag '5F57' is dedicated to this data element. Account Type is applicable for Service Pack 2 and onward.

Table 2-15.1 - Account Type

Value	Account Type
'00'	Default – unspecified
'10'	Savings
'20'	Cheque/debit
'30'	Credit
All other values RFU	

2-15.2.2 Account Type Selection

Purpose: To indicate whether Account Type selection is allowed.

Format: 1 byte binary.

Contents: '00' - Account Type Selection is not allowed
'FF' - Account Type Selection is allowed.

Remarks: Found in the Swedish Processing Condition Table, table 1-15.6 page 1-15-16.

2-15.2.3 Acquirer Name

Purpose: To indicate the name of the Acquirer that will process this transaction.

Format: ans24 (24 bytes)

Contents: A textual description of the Acquirer that will handle the transaction.

Remarks: Found in the (Swedish) Processing Condition Table, table 1-15.6 page 1-15-16.

2-15.2.4 Action Code

Reference: Ref. 25: "APACS Standard 60", and ref. 11: "ISO 8583:1993".

Purpose: To inform the CAD of the transaction result. It is generated by the host and/or PSAM.

Format: n4 (2 bytes).

Contents: See section 2-13.9.9 page 2-13-82.

Remarks: The Action Code is transmitted in field 39 in APACS 60 messages.

2-15.2.5 Action Indicator

- Purpose:** To indicate for the PSAM which security actions to be taken subsequently. The indication is based upon the external kernel decisions.
- Format:** b2 (2 bytes).
- Contents:** See table 2-15.2 for the contents of the least significant byte (LSB). MSB is reserved for future use.
- Remarks:** The data element Action Indicator is provided to the PSAM in the *Initiate Contactless Payment* command. Action Indicator is part of the enciphered data using the KSES_{CDP}.

Table 2-15.2 - Coding of Action Indicator (LSB)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	x	x	x	<u>CVM handling:</u>
-	-	-	-	-	0	0	0	- No CVM
-	-	-	-	-	0	0	1	- Signature
-	-	-	-	-	0	1	0	- Online PIN
-	-	-	-	-	0	1	1	- On Device CVM/Consumer Device CVM
-	-	-	-	-	1	x	x	- RFU
-	-	-	-	x	-	-	-	<u>Online/Offline:</u>
-	-	-	-	0	-	-	-	- Offline
-	-	-	-	1	-	-	-	- Online
-	-	x	x	-	-	-	-	<u>Kernel Result:</u>
-	-	0	0	-	-	-	-	- Approved
-	-	0	1	-	-	-	-	- Declined, unconditional
-	-	1	0	-	-	-	-	- Declined, new technology recommended
-	-	1	1	-	-	-	-	- RFU
x	x	-	-	-	-	-	-	RFU

2-15.2.6 Addendum Record

- Purpose:** To hold additional information.
- Format:** LEN_{ADD} bytes.
- Contents:** Any.
- Remarks:** See section 2-13.9.21 page 2-13-94 for more details.

2-15.2.7 AID (Application Identifier)

- Reference:** Ref. 9: "ISO/IEC 7816-5" and ref. 20: "EMV ICC Specification" (tag='4F')
- Purpose:** To identify an application in an IC Card.
- Format:** b5-16 (5-16 bytes).
- Contents:** An AID consists of a registered Application Identifier (RID) optionally followed by a Proprietary Application Identifier Extension (PIX). The RID is 10 hexadecimal characters long, e.g.:
 Dankort: 'A000000121'
 Visa: 'A000000003'
 MasterCard: 'A000000004'
 Europay: 'A000000010'
 while the PIX consists of up to 22 hexadecimal characters. Currently, the PIX values specified by Europay and MasterCard are four digits long.
- Remarks:** The data element that identifies the AID (tag '4F') of an application is the DF Name (tag '84') of this application. The RID extracted from this AID is used to find/identify the Certification Authority Public Key.

2-15.2.8 Algorithm Id

Purpose: To indicate the algorithm used for hash computation to be used in Electronic Receipts.

Format: b1 (1 byte).

Contents: See table 2-15.3.

Table 2-15.3 - Defined Algorithms

Value	Algorithm	Input	Description
'00'	SHA256	PAN only	SHA256(PAM Salt) = Hash value
'01'..'FF'	To be defined	To be defined	To be defined

2-15.2.9 ALG_{VLP}

Purpose: To indicate the algorithm used for local PIN verification.

Format: b1 (1 byte).

Contents: At the discretion of the Terminal Supplier and his client.

2-15.2.10 ALG_{VPPSYNC} (Synchronization Algorithm and Key Length)

Purpose: To identify both algorithm (DES/DEA, AES, ...) and key length to be used for PED/PSAM key synchronization..

Format: b1 (1 byte).

Contents: The following values are currently defined:

- '01': 2TDEA (triple-DES with a double-length key of 112 bits + parity)
- '02': 3TDEA (triple-DES with a triple-length key of 168 bits + parity)
- '11': AES-128 (for future use)
- '12': AES-192 (for future use)
- '13': AES-256 (for future use).

Remarks: The left-most half-byte identifies the algorithm and the right-most half-byte defines the key length. Only '01' (2TDEA) will be supported in the first implementations of the PSAM and Host systems. '02' (3TDEA) is not likely to be supported ever. Instead, AES will probably be used in future versions.

2-15.2.11 Amount

Purpose: To indicate the transaction amount to the involved components, such as PSAM, Terminal Operator/acquirer hosts and EMV card.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: Amount is provided by the Merchant Application and forwarded by the MAD-Handler to the PSAM. The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units.

2-15.2.12 Amount, Other

Purpose: To hold a cashback amount.

Format: b4 (4 bytes).

Contents: Amount, Other is coded identically to Amount (see section 2-15.2.11 page 2-15-4).

2-15.2.13 Amount Request

- Purpose:* To indicate whether the amount to be requested in the *Get Amount 3* command is the initial amount or final amount.
- Format:* b1 (1 byte).
- Contents:* '00' = Initial Amount Request (Estimated or Accurate)
'FF' = Final Amount Request (Accurate)

2-15.2.14 Amount Status

- Purpose:* To indicate whether the amount returned in the *Get Amount 3* command is the estimated or accurate amount.
- Format:* b1 (1 byte).
- Contents:* '00' = Estimated Amount
'FF' = Accurate Amount

2-15.2.15 Application Label

- Reference:* Ref. 9: "ISO/IEC 7816-5" and ref. 20: "EMV ICC Specification" (tag='50')
- Purpose:* Mnemonic associated with the AID.
- Format:* an1..16. Characters coded according to ref. 12: "ISO/IEC 8859-15".
- Contents:* Alpha and numeric characters.

2-15.2.16 Approval Code

- Purpose:* Response identification assigned by the authorizing institution (or its agent). This is commonly referred to as the authorization code.
- Format:* anp6 (6 bytes) or b6 (with the value '00 00 00 00 00 00').
- Contents:* At the discretion of the authorizing institution.
- Remarks:* In the response to the *Validate Data 2* command, the following binary values are used as an indication of "not available" and should be handled as space filled.
- Zero filled: '00 00 00 00 00 00'
 - Space filled: '20 20 20 20 20 20' (in the response to the Check Stop List command)
 - FF filled: 'FF FF FF FF FF FF' (normally during Tokens captures)

2-15.2.17 ASI (Application Selection Indicator)

- Reference:* Ref. 20: "EMV ICC Specification".
- Purpose:* The terminal uses the ASI to determine whether exact match between the ADF name in the card and the AID in the terminal is required or whether a partial match is allowed.
- Format:* b1 (1 byte).
- Contents:* '00' = Partial match of the AID is allowed
'FF' = Exact match between the ADF name in the card and the AID in the terminal is required.
- Remarks:* The value of the Application Selection Indicator is given in the response to the *Get Debit/Credit Properties* command.

2-15.2.18 Available Funds

- Purpose:* To indicate the amount available for the next charge of the card. The Available Funds is always associated with a sign, either "C" (indicating +) or "D" (indicating -) both in ASCII format.
- Format:* X + b4 (4 bytes) where X indicates the sign.
- Contents:* Amount is coded as an unsigned binary integer.
- Remarks:* The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. The Available Funds can be obtained from the response to the *Validate Data 2* command. If Available Funds is absent from the host, all 5 bytes will be filled with 'F's.

2-15.2.19 AOSA (Available Offline Spending Amount)

- Purpose:* To indicate the accumulated amount available for spending until online next time.
- Format:* b6 (6 bytes) BCD coded.
- Contents:* Amount is coded as an unsigned binary integer in minor currency unit.
- Remarks:* This is a Visa payWave specific requirement. The value is, when available, returned as tag '9F5D' from the card to the POS system. The value shall be displayed and or printed on the receipt. The terminal shall process the data in the following way:
- Strip off leading zeroes
 - Prefix or suffix the currency indicator
 - Insert decimal place as applicable to the currency.
- The presence of the feature is issuer dependent.

2-15.2.20 Batch Number

- Purpose:* To group certain transactions for settlement. The batch number is applicable for Financial, Addendum and Reversal transactions and is maintained by the merchant. Only a single currency is allowed in one batch.
- Format:* anp12 (12 bytes).
- Contents:* At the discretion of the merchant.

2-15.2.21 BIB

- Purpose:* To indicate whether banking transactions are allowed ("Bank i Butik " i.e. bank in shop functions).
- Format:* 1 byte binary.
- Contents:* '00' - Banking transactions are not allowed
'FF' - Banking transactions are allowed.
- Remarks:* Found in the (Swedish) Processing Condition Table, table 1-15.6 page 1-15-16.

2-15.2.22 BIB Amount

- Purpose:* To indicate the maximum transaction amount when performing banking transactions.
- Format:* b4 (4 bytes).
- Contents:* Found in the Swedish Processing Condition Table, table 1-15.6 page 1-15-16. A value of 0 indicates unlimited transaction amount.
- Remarks:* The value represents the lowest denominator for the corresponding Currency Code, e.g. for SEK, amounts are represented in 1/100 SEK units.

2-15.2.23 BIB Processing Code

Purpose: To indicate transaction type for banking services in the terminal.

Format: n2 (1 byte).

Contents: '14' - Cash at ME
'21' - Deposit
'28' - Deposit at ME.

Remarks: None.

2-15.2.24 Card Data

Purpose: To hold card data in a Key Entered transaction.

Format: b (Variable length).

Contents: PAN || Expiry Date || CV-2

Remarks: Example: 5019994000107021 1214 F848 where
PAN = 5019994000107021
Expiry Date = 1214 in the format MMY from the surface of the card
CV-2 = F848 (note the leading 'F' if only 3 digits are used).

2-15.2.25 [Card Data]

Purpose: To hold enciphered card data in a Key Entered transaction. The Card Data listed below are enciphered by the session key $KSES_{CDP}$.

Format: b (Variable length, up to 24 bytes.).

Contents: Random Number (4 bytes) || PAN (up to 10 bytes) || Expiry Date (2 bytes) || CV-2 (2 bytes) || Padding

Remarks: This data element is applicable when Card Data Protection is supported and a Key Entered transaction is performed.
Padding according to ref. 15: "ISO/IEC 9797", Padding method 2.

2-15.2.26 Card Data Source

Purpose: To indicate the source of card data.

Format: b1 (1 byte)

Contents:

'00'	EMV
'01'	MSC
'02'	Key entered
'03'	Token
'04'	Contactless
'05'..'43'	RFU
'44'	Contactless ICC (External kernel)
'45'	Contactless MSD (External Kernel)
'46'..'FF'	RFU

2-15.2.27 Card Name

Purpose: The official name of the card to be printed on the cardholder's receipt.

Format: ans16 (16 bytes).

Contents: Characters coded according to ref. 12: "ISO/IEC 8859-15".

Remarks: Trailing blanks are used for padding.

2-15.2.28 Card Product Type

Purpose: To indicate the card product type for given AID.

Format: b2 (2 bytes).

Contents: See table 2-15.4 and 2-15.5.

Remarks: This data element has been defined as tag 'DF72'. Card Product Type can be obtained by issuing the *Get D/C Properties* command with Identifier = '0009'. The unused bits (RFU) are set to zero.

Table 2-15.4 - Byte 1 (MSB) of Card Product Type

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	<u>Debit:</u>
-	-	-	-	-	-	-	0	- Debit not supported
-	-	-	-	-	-	-	1	- Debit supported
-	-	-	-	-	-	x	-	<u>Credit:</u>
-	-	-	-	-	-	0	-	- Credit not supported
-	-	-	-	-	-	1	-	- Credit supported
-	-	-	-	-	x	-	-	<u>Prepaid ICC:</u>
-	-	-	-	-	0	-	-	- Prepaid ICC not supported
-	-	-	-	-	1	-	-	- Prepaid ICC supported
-	-	-	-	x	-	-	-	<u>Gift card ICC:</u>
-	-	-	-	0	-	-	-	- Gift card ICC not supported
-	-	-	-	1	-	-	-	- Gift card ICC supported
x	x	x	x	-	-	-	-	RFU

Table 2-15.5 - Byte 2 (LSB) of Card Product Type

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	RFU

2-15.2.29 Card Reference

Purpose: The Card Reference is a unique value based upon the PAN. The unique value is computed by use of a cryptographic algorithm.

Format: b8 (8 bytes).

Contents: Unique card reference.

Remarks: The Card Reference can be retrieved in the *Submit Card Reference* command issued by the PSAM. The data element is supplementary to element 2-15.2.53 Dual Card Reference.

2-15.2.30 Card Sequence Number

Purpose: Identifies and differentiates cards with the same PAN. Used in the APACS message (Field 23).

Format: n3 (2 bytes).

Contents: BCD coded.

Remarks: PAN Sequence Number is a similar data element used in EMV context. Padded with leading zero.

2-15.2.31 Card Service Info

Purpose: To indicate specific card information, which may be relevant for the terminal. This information are maintained by the PSAM. The unused bits (RFU) are set to zero.

Format: b1 (1 byte).

Contents: See table 2-15.6.

Table 2-15.6 - Coding of Card Service Info

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	x	x	<u>Reserved for PSAM usage:</u>
–	–	–	–	–	x	–	–	<u>Service Code¹⁾:</u>
–	–	–	–	–	0	–	–	– Service Code <i>not</i> accessible
–	–	–	–	–	1	–	–	– Service Code accessible
x	–	–	–	–	–	–	–	<u>Private Label Card Scheme:</u>
1	–	–	–	–	–	–	–	– The card (and the PAN) may be used for a private label card scheme applications.
–	–	–	–	–	–	–	–	– The card (and the PAN) must <i>not</i> be used for a private label card scheme applications.
–	x	–	–	–	–	–	–	<u>Card Processing:</u>
–	1	–	–	–	–	–	–	– The card (and the PAN) can <i>not</i> be processed by the PSAM.
–	–	–	–	–	–	–	–	– The card (and the PAN) can be processed by the PSAM.
–	0	–	–	–	–	–	–	
–	–	–	–	–	–	–	–	
–	–	x	–	–	–	–	–	<u>Expiry Status²⁾:</u>
–	–	1	–	–	–	–	–	– The track is expired.
–	–	0	–	–	–	–	–	– The track is not expired.
–	–	–	x	x	–	–	–	RFU
Legend:								
1) The Service Code is a don't care value, returned as 0, when performing the <i>Retrieve Card Data</i> command.								
2) Expiry Status is a don't care value, returned as 0, when it is a Private Label Card Scheme.								

2-15.2.32 Cashback

Purpose: To indicate that cashback is allowed for this PAN.

Format: b1 (1 byte).

Contents: '00' - Cashback is not allowed
'FF' - Cashback is allowed.

Remarks: Found in the Processing Condition Table, table 1-10.5 page 1-10-28.

2-15.2.33 CNT_x (Count of X)

Purpose: To inform the CAD of the number of data elements or structures of a given type that follow.

Format: b1 (1 byte).

Contents: The number of data elements/structures to follow coded as an unsigned binary integer.

Remarks: Examples of use are CNT_{ENTRIES}, CNT_{MSC}, and CNT_{H1H2}.

2-15.2.34 Contactless Terminal Settings

Purpose: To indicate to the terminal a number of parameters related to a specific AID.

Format: b4 (4 bytes).

Contents: See table 2-15.7 for the coding.

Remarks: Whether the Cashback is controlled by the terminal/ECR or the PSAM Administrative System, the most restrictive decision is decisive i.e. if one of the entities indicates that Cashback is not allowed, Cashback is not allowed. Bits b9 – b32 are RFU.

Table 2-15.7 - Coding of Contactless Terminal Settings (LSB)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	x	x	<u>Soft/Hard Limit market:</u>
-	-	-	-	-	-	0	0	- Normal
-	-	-	-	-	-	0	1	- Hard Limit
-	-	-	-	-	-	1	0	- Soft Limit
-	-	-	-	-	-	1	1	- RFU
-	-	-	-	-	x	-	-	<u>Cashback:</u>
-	-	-	-	-	0	-	-	- Not allowed
-	-	-	-	-	1	-	-	- Allowed
-	-	-	-	x	-	-	-	<u>Partial/full match on AID:</u>
-	-	-	-	0	-	-	-	- Partial match
-	-	-	-	1	-	-	-	- Full match
-	-	-	x	-	-	-	-	<u>Status Check:</u>
-	-	-	0	-	-	-	-	- Not supported
-	-	-	1	-	-	-	-	- Supported
-	-	x	-	-	-	-	-	<u>Zero Amount:</u>
-	-	0	-	-	-	-	-	- Not allowed
-	-	1	-	-	-	-	-	- Allowed
x	x	-	-	-	-	-	-	RFU

2-15.2.35 CURRC (Currency Code)

Reference: Ref. 1: "ISO 4217" and ref. 12: "ISO/IEC 8859-15".

Purpose: To indicate the numeric code for the currency used in the transaction.

Format: n3 (2 bytes).

Contents: The 3-digit numeric currency codes are used except for printing and display purposes.

Remarks: The numeric Currency Code for the Danish currency is 208 and the alphabetic Currency Code is "DKK". When the Currency Code is displayed or printed, it is displayed/printed in the corresponding alpha-characters according to ref. 12: "ISO/IEC 8859-15". Padded with leading zero.

2-15.2.36 CURRE (Currency Exponent)

Purpose: To indicate the implied position of the decimal point from the right of the transaction Amount.

Format: n1 (1 byte). Ref. 1: "ISO 4217".

Contents: 1 digit.

2-15.2.37 CV-2 (Card Verification, method 2)

Purpose: To give a higher degree of security when performing Key Entered transactions. The scheme independent name is Card Security Code. CV-2 (called CVV-2, CVC-2 and CID by Visa, MasterCard and American Express) is printed in the signature panel of a card but is not included in the magnetic stripe.

Format: n4 (2 bytes).

Contents: BCD coded. If only 3 digits are used, a leading 'F' is used as padding, e.g. 'F848'. If empty filled with 'FFFF'.

Remarks: Part of the Card Data used for Key Entered transactions. Please note that some American Express cards are using 4 digits.

2-15.2.38 CVM Status

Purpose: To indicate which type(s) of CVM that is required to perform the transaction.

Format: b1 (1 byte).

Contents: See table 2-15.8.

Table 2-15.8 - Coding of CVM Status

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	x	x	<u>PIN:</u>
-	-	-	-	-	-	x	0	- PIN <i>not</i> verified
-	-	-	-	-	-	0	1	- PIN verified offline
-	-	-	-	-	-	1	1	- PIN (to be) verified online
-	-	-	-	-	x	-	-	<u>Signature:</u>
-	-	-	-	-	0	-	-	- Signature <i>not</i> requested
-	-	-	-	-	1	-	-	- Signature requested
-	-	-	-	x	-	-	-	<u>Authorization:</u>
-	-	-	-	0	-	-	-	- Offline
-	-	-	-	1	-	-	-	- Online
-	-	-	x	-	-	-	-	<u>Fallback:</u>
-	-	-	0	-	-	-	-	- Fallback transaction <i>not</i> initiated
-	-	-	1	-	-	-	-	- Fallback transaction initiated
-	-	x	-	-	-	-	-	<u>On Device CVM/Consumer Device CVM:</u>
-	-	0	-	-	-	-	-	- Device CVM <i>not</i> performed
-	-	1	-	-	-	-	-	- Device CVM performed
x	x	-	-	-	-	-	-	RFU

Remarks: The unused bits (b8 - b7) shall be set to zero.
If the terminal tries to go online, but receives no response from the host, two cases occur concerning the "Offline/Online" bit (b4): if the transaction is finished successfully offline, the bit b4 will be reset. If the transaction is rejected (and a Reversal Advice is generated), the bit b4 remains set, indicating the intention.

2-15.2.39 Data Requested

Purpose: To indicate which data is requested.

Format: b1 (1 byte).

Contents: '00' Token related data
'01' - 'FF' Reserved for Future Use

Contents: See table 2-15.9.

Table 2-15.9 - Coding of Data Requested

Value	Meaning
'00'	Token related data
'01'..'FF'	RFU

2-15.2.40 DATE_{PCT}

Purpose: To specify the date of creation the Processing Condition Table.

Format: n6 (3 bytes).

Contents: Six digits representing YYYYMMDD.

Remarks: Found in the generic Processing Condition Table, table 1-10.5 page 1-10-28.

2-15.2.41 DCC Amount Extra (CH)

Purpose: To indicate the additional amount added by the cardholder, e.g. gratuity.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. If DCC is chosen by the cardholder, the cardholder may add an extra amount (gratuity) in the cardholders home currency. In this case the total in the Merchants local currency "Amount Total (ME)" shall be adjusted accordingly.
If no extra amount is added, the data element shall be filled with zeroes.

2-15.2.42 DCC Amount Goods & Services (ME)

Purpose: To indicate the transaction amount in Merchant local currency inclusive Surcharge and other extra charges, but exclusive Extra added in the Cardholders Billing currency.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units.

2-15.2.43 DCC Amount Total (ME)

Purpose: To indicate the total transaction amount in Merchant local currency inclusive Surcharge and Extra.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units.

DCC Amount Total (ME) shall contain the Total Amount, i.e. amount paid for goods/services, any merchant decided surcharges, and extra/gratuity added by cardholder. The extra/gratuity amount is computed from the corresponding value in the Cardholders Billing Currency: DCC Amount Extra (CH).

2-15.2.44 DCC Commission (CH)

Purpose: To indicate the additional commission amount in the cardholders home currency.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. DCC Commission (CH) is not included in the total amount (DCC Amount Total (CH) as DCC Commission (CH) is part of the DCC calculation process/formula.

If a fixed DCC commission in the cardholders billing currency is added, this value shall be indicated in the data element DCC Commission (CH). If no DCC Commission is added, the data element shall be filled with zeroes.

2-15.2.45 DCC Commission (ME)

Purpose: To indicate the additional commission amount in Merchants local currency.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. If a fixed DCC commission in the Merchants local currency is added, this value shall be indicated in the data element DCC Commission (ME).

DCC Commission (ME) is not included in the total amount (DCC Amount Total (ME) as DCC Commission (ME) is part of the DCC calculation process/formula.

If no DCC Commission is added, the data element shall be filled with zeroes.

2-15.2.46 DCC CURR (ME)

Purpose: Identifies the currency for a transaction in Merchant local currency.

Format: n6 (3 bytes).

Contents: DCC CURR contains both the Currency Code and the Currency Exponent. 3 bytes BCD in the form '0c cc 0e', where ccc is the code assigned to the currency by ref. 1: "ISO 4217", and e is the exponent.

2-15.2.47 DCC Indicator

Purpose: To indicate the actual DCC implementation and by this the actual DCC algorithm.

Format: n4 (2 bytes).

Contents:

Remarks: The value for DCC Indicator is defined by Nets.

2-15.2.48 DCC Mark Up Exchange Rate

Purpose: To indicate the Mark Up on currency reference exchange rate between Merchants local currency and cardholders home currency.

Format: n8 (4 bytes).

Contents: The leftmost digit denotes the number of positions the decimal separator shall be moved from the right. Position 2-8 is the rate, e.g., a conversion

rate value of 91234567 would equate to 0,001234567.
The maximum number of digits to the right of the decimal separator is 9, provided the first two digits to the right of the decimal separator are zeroes according to ref. 11: "ISO 8583/1993", section 4.4.14.

Remarks: In order to obtain the highest level of accuracy, the value contained in position 2-8 shall aim to include 7 significant digits, i.e. no leading zero in position 2-8.

2-15.2.49 DCC Reference Exchange Rate

Purpose: To indicate the reference currency exchange rate between Merchant local currency and cardholders home currency.

Format: n8 (4 bytes).

Contents: The leftmost digit denotes the number of positions the decimal separator shall be moved from the right. Position 2-8 is the rate, e.g., a conversion rate value of 91234567 would equate to 0,001234567.
The maximum number of digits to the right of the decimal separator is 9, provided the first two digits to the right of the decimal separator are zeroes according to ref. 11: "ISO 8583/1993", section 4.4.14.

Remarks: In order to obtain the highest level of accuracy, the value contained in position 2-8 shall aim to include 7 significant digits, i.e. no leading zero in position 2-8.

2-15.2.50 DCC Reference Date

Purpose: To indicate the date related to reference exchange rate.

Format: n8 (4 bytes).

Contents: YYYY MM DD

2-15.2.51 DCC Waiter ID

Purpose: To indicate the information about the waiter receiving the DCC Amount Extra

Format: b1 (1 byte).

Contents: Value in the range 0 to 255. If the information is not available or relevant, the field shall be zero filled.

Remarks: In order to obtain the highest level of accuracy, the value contained in position 2-8 shall aim to include 7 significant digits, i.e. no leading zero in position 2-8.

2-15.2.52 Default Kernel ID

Purpose: To indicate a default Kernel ID for a matching AID in case that the Kernel Identifier (Tag '9F2A') is absent.

Format: b1 (1 byte).

Contents: See table 2-15.10 for the values.

Remarks: If the length of the Kernel Identifier value field is zero, then Entry Point shall use a default value for the Requested Kernel ID, based on the matching AID, as indicated in table 2-15.10.

Table 2-15.10 - Default Value for Requested Kernel ID

Matching AID		Default Value for Requested Kernel ID
MasterCard	RID: A0 00 00 00 04	B' 00000010
Visa	RID: A0 00 00 00 03	B' 00000011

2-15.2.53 Dual Card Reference

Purpose: The Dual Card Reference is a set of (up to) two unique values, a primary value and a secondary value. The values are computed by use of a cryptographic algorithm. See table 2-15.11 for further information.

Format: b16 (16 bytes).

Contents: Two unique card references.

Remarks: The Dual Card Reference can be retrieved by use of the the following commands:

- *Submit Card Reference 2* command
- *Retrieve Card Data* command (MSC)
- *Retrieve Card Data* command (EMV) requesting tag 'D4'

The Dual Card Reference is an extension of Card Reference. Dual Card Reference is computed only in the case where the number of PAN digits are in the range 10 – 19 digits.

Table 2-15.11 - Dual Card Reference

Card Data Source	Dual Card Reference based upon:	
	Primary Value	Secondary Value
EMV	PAN, PAN Sequence Number ¹⁾ & Expiry Date	PAN
MSC	Track 2 ²⁾	PAN
Legend:		
1)	If present. If absent the Card Reference is computed using the PAN FF Expiry Date as basis.	
2)	The primary value will be set to '00 00 00 00 00 00 00 00'.	

2-15.2.54 Duplicate Transaction Time-out

Purpose: To indicate a time frame in which two subsequent transactions, involving the same PAN and amount, results in a rejection of the later. When the value is different from zero, this check (performed by the PSAM) prevents duplicate successful transactions.

Format: b1 (1 byte).

Contents: '00' No check of duplicate transactions is performed.
'01' - 'FF' Number of minutes (1 - 255) in which a check of duplicate transactions is active.

Remarks: The duplicate check is applicable for transactions with financial impact only (Purchase, Refund and Capture).
The value is set utilizing the *Set Debit/Credit Properties* command with identifier '8002'.
Default value is 10 minutes.

2-15.2.55 EMV Checksum

Purpose: To uniquely identify the actual terminal implementation.

Format: b8 (8 bytes).

Contents: A checksum calculated on the Terminal Checksum, PSAM Code Checksum and PSAM Config Checksum.

Remarks: The EMV Checksum shall be displayed/printed as 16 hexadecimal digits. This checksum is identical only for terminals from one vendor with the same configuration (including the same PSAM version).

2-15.2.56 Error Code

Purpose: To indicate for the PSAM any irregularities discovered during the kernel processing of a contactless transaction.

Format: b2 (2 bytes).

Contents: See table 2-15.12.

Remarks: The data element Error Code is provided to the PSAM in the *Initiate Contactless Payment* command. The PSAM will convert the Error Code to a specific Application Status Word (ASW1-ASW2). The ASW1-ASW2 is conveyed in field 46, Tag TK.

Table 2-15.12 - Error Codes

Error Code	Description	ASW1-ASW2
'0000'	Successful	'0000'
'1000'	Terminal error	'1800'
'1001'	Pre-processing error	'1801'
'1002'	PPSE error	'1802'
'1003'	Select error	'1803'
'1004'	Card present, but power-up fails	'1804'
'1005'	Protocol activation error	'1805'
'1006'	Terminal missing data	'1806'
'1007'	Card not present/Card removed	'1807'
'1008'	Transaction aborted by application/merchant	'1808'
'1009'	Previous transaction not finished	'1809'
'2000'	Kernel error	'1810'
'2001'	Offline declined	'1811'
'2002'	ICC missing data	'1812'
'2003'	ICC redundant data	'1813'
'2004'	ICC data format error	'1814'
'2005'	Use contact interface	'1815'
'2006'	Expired certificate	'1816'
'2007'	Revoked certificate	'1817'
'2008'	Kernel not available	'1818'
'2009'	Communication error	'1819'
'200A'	Error in input parameters	'181A'

2-15.2.57 Expiry Date

Reference: Ref. 20: "EMV ICC Specification" (Application Expiration Date, tag='5F24').

Purpose: To indicate the date of expiration for the card (or application).

Format: n4 (2 bytes).

Contents: Four digits representing YYYY.

2-15.2.58 Expiry Date (Surface of the Card)

- Purpose:* To indicate the date of expiration for the card (or application).
- Format:* n4 (2 bytes).
- Contents:* Four digits representing MMY Y.
- Remarks:* Part of the Card Data used for Key Entered transactions.

2-15.2.59 Extended Issuer Envelope Data

- Purpose:* To hold additional acquirer/issuer related data conveyed transparently to the acquirer/issuer e.g. Merchant reference number.
- Format:* b..nnn (nnn bytes).
- Contents:* At the discretion of the Acquirer/Issuer.
- Remarks:* When the Extended Issuer Envelope Data is conveyed during a transaction, the total number of bytes in the APACS message is the limiting factor. A *Get Debit/Credit Properties* command with identifier = '0011' can return the total space available for Issuer Envelope Data and the Extended Issuer Envelope Data together.

2-15.2.60 FILEID_{ADMIN}

- Purpose:* Identifies the administrative file that is stored in the Data Store.
- Format:* 2b (2 bytes).
- Contents:* Unique file identifier.
- Remarks:* Zero filled if the administrative file is not used.

2-15.2.61 FILEID_{PRIORITY,n}

- Purpose:* Identifies the priority files that is stored in the Data Store.
- Format:* (2*n)b.
- Contents:* Unique file identifier.
- Remarks:* "n" identifies the number of priority files.

2-15.2.62 Final Card Balance

- Purpose:* To indicate the card balance of a prepaid ICC/contactless card *after* a purchase transaction has been performed.
- Format:* b4 (4 bytes).
- Contents:* Amount is coded as an unsigned binary integer.
- Remarks:* The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. Part of the *Initial Contactless Payment* command response or the *Validate Data 2* command response.

2-15.2.63 Hardware Version Number

- Purpose:* To indicate the version number of the terminal hardware.
- Format:* b2 (2 bytes).
- Contents:* At the discretion of the Terminal Supplier. A new hardware version should, however, have an increased version number.

2-15.2.64 Host Request

Purpose: To hold a host request message.

Format: LEN_{HREQ} bytes.

Contents: Any.

Remarks: Host Request is supplied by the Nets PSAM.

2-15.2.65 Host Response

Purpose: To hold host response data.

Format: LEN_{HR} bytes.

Contents: Any.

2-15.2.66 ID_{PSAM} (Identifier for a PSAM)

Purpose: To uniquely identify each PSAM

Format: b4 (4 bytes).

Contents: At the discretion of the PSAM Creator

2-15.2.67 ID_{PSAMAPP} (TAPA PSAM Application Identifier)

Purpose: To identify a particular PSAM application.

Format: b2 (2 bytes).

Contents: '8111' indicates Nets Debit/Credit application according to this specification.

2-15.2.68 ID_{PSAMCREATOR}

Purpose: Identify the creator of the PSAM. Ref. 27: "TAPA, Application Architecture Specification".

Format: b4 (4 bytes).

Remarks: Assigned by the owner of the RID_{PSAM}.

2-15.2.69 Info Level

Purpose: To indicate which type(s) of information the PSAM shall provide to the Merchant Application.

If Merchant Application Log is required, a slightly modified (field 25) copy of the advice sent to the Data Store will additionally be sent to the Merchant Application for backup purposes.

If State information is requested, the PSAM will indicate to the Merchant Application the progress during the transaction, e.g. 'Waiting for amount'.

Format: b1 (1 byte).

Contents: See table 2-15.13.

Table 2-15.13 - Coding of Info Level

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	–	x	<u>Merchant Application Log:</u>
–	–	–	–	–	–	–	0	– Log info <i>not</i> requested
–	–	–	–	–	–	–	1	– Log info requested
–	–	–	–	–	–	x	–	<u>Transaction State Information:</u>
–	–	–	–	–	–	0	–	– Status is <i>not</i> requested
–	–	–	–	–	–	1	–	– Status is requested
–	–	–	–	–	x	–	–	<u>Original/Extended Authorization:</u>
–	–	–	–	–	0	–	–	– Confirm Amount is <i>not</i> requested
–	–	–	–	–	1	–	–	– Confirm Amount is requested
x	x	x	x	x	–	–	–	RFU

Remarks: The unused bits (b8 - b4) shall be set to zero.

2-15.2.70 Initial Card Balance

Purpose: To indicate the card balance of a prepaid ICC/contactless card *before* a purchase transaction has been performed.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. Part of the *Initial Contactless Payment* command response or the *Validate Data 2* command response.

2-15.2.71 Issuer DD (Issuer Discretionary Data in FCI)

Reference: Ref. 20: "EMV ICC Specification" (File Control Information (FCI) Issuer Discretionary Data, tag='BF0C').

Purpose: To hold the FCI Issuer Discretionary Data in the response to the *Select* command.

Format: Binary, variable length.

Contents: At the discretion of the Issuer.

2-15.2.72 Issuer Envelope Data

Purpose: To hold issuer related data conveyed transparently to the issuer e.g. loyalty related data.

Format: b..150 (150 bytes).

Contents: At the discretion of the Issuer.

Remarks: When the Issuer Envelope Data is conveyed during a transaction, the number of bytes are limited to 150 bytes.

2-15.2.73 Kernel ID

Purpose: Indicates the card's preference for the kernel on which the contactless application can be processed. If absent, the default Kernel ID shall be used.

Format: b1 (1 byte).

Contents: See table 2-15.14.

Remarks: Tag '9F2A'. The data element Kernel ID is provided to the PSAM in the *Get Tag List for External Kernel* command. Example: A *payWave* kernel ID will be coded as: '00000011'. A *PayPass* kernel ID will be coded as: '00000010'.

Table 2-15.14 - Coding of Kernel ID

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Type of kernel:
0	0							An international kernel, with a kernel identifier assigned by EMVCo and coded in Short Kernel ID
0	1							RFU
1	0							A domestic kernel, with kernel identifier in EMVCo format, coded by the concatenation of the short Kernel ID and the Extended Kernel ID
1	1							A domestic kernel, with kernel identifier in proprietary format, coded by the concatenation of the short Kernel ID and the Extended Kernel ID
		x	x	x	x	x	x	Short Kernel ID:
		0	0	0	0	0	0	The kernel is associated with the corresponding ADF Name
		0	0	0	0	0	1	JCB Kernel (Kernel 1)
		0	0	0	0	1	0	PayPass kernel (Kernel 2)
		0	0	0	0	1	1	payWave kernel (Kernel 3)
		0	0	0	1	0	0	American Express kernel (Kernel 4)
		0	0	0	1	0	1	5 th kernel
		-	-	-	-	-	-	
		1	1	1	1	1	1	63 rd kernel

2-15.2.74 Kernel Version

Purpose: To indicate for the PSAM the current version of the kernel.

Format: b2 (2 bytes).

Contents: Kernel version converted to hexadecimal (see example below).

Remarks: The data element Kernel version is provided to the PSAM in the *Get Tag List for External Kernel* command. Example: Version 2.0.2 will be represented as '00CA'.

2-15.2.75 Key Check Value (KCV)

Purpose: To verify the status of the session key shared between a PSAM and a PIN Pad.

Format: b3 (3 bytes).

Contents: The 3 most significant bytes of the result of a triple-DES encryption of an 8-byte block of binary zeros.

Remarks: The subscript indicates whether the PSAM or the PIN Pad has computed the KCV.

2-15.2.76 Key Enter

- Purpose:** To indicate whether key entering of the card data is allowed.
- Format:** 1 byte binary.
- Contents:** '00' - Key entering is not allowed
'FF' - Key entering is allowed.
- Remarks:** Found in the Processing Condition Table, table 1-10.5 page 1-10-28.

2-15.2.77 LEN_x (Length of Field X)

- Purpose:** To indicate the length of the following data element or structure.
- Format:** b1 or b2.
- Contents:** The length coded as an unsigned binary integer. The value '00' or '0000' indicates that the corresponding data element/structure is absent.
- Remarks:** Examples of use are: LEN_{ADD}, LEN_{AdditionalInfo}, LEN_{AID}, LEN_{AMOUNTS}, LEN_{AT}, LEN_{CARDDATA}, LEN_{DATA}, LEN_{HR}, LEN_{HREQ}, LEN_{IDD}, LEN_{MDOL1}, LEN_{MDOL2}, LEN_{PAN}, LEN_{PDOL}, LEN_{STAT}, LEN_{TOKEN}, LEN_{TRACK2}, LEN_{UPD}.

2-15.2.78 Limit Info

- Purpose:** To indicate for the PSAM how the Floor Limit, CVM Required Limit and Transaction Limit shall be interpreted in respect to Soft Limit or Hard Limit markets (Maestro *PayPass*).
- Format:** b1 (1 byte).
- Contents:** See table 2-15.15.
- Remarks:** The "Normal" setting in table 2-15.15 will typically be used for Visa AIDs.

Table 2-15.15 - Coding of Limit Info

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	x	x	<u>Soft/Hard Limit market:</u>
-	-	-	-	-	-	0	0	- Normal
-	-	-	-	-	-	0	1	- Hard Limit
-	-	-	-	-	-	0	0	- Soft Limit
-	-	-	-	-	-	0	1	- RFU
x	x	x	x	x	x	-	-	RFU

2-15.2.79 Local PIN Verification Status

- Purpose:** To indicate the success or failure of local PIN verification.
- Format:** b1 (1 byte).
- Contents:** '00' Successful
'FF' PIN rejected.
- Remarks:** Values other than the specified are not valid. Part of the response to *Verify Local PIN* command.

2-15.2.80 MAD-Handler ID

- Purpose:** Unique identifier of the terminal equipment (or more specifically, the MAD-Handler).
- Format:** ans8.
- Contents:** Terminal Manufacturer ID (3 bytes) || Terminal Serial Number (5 bytes).
- Remarks:** The MAD-Handler ID is conveyed to the host in field 46 (CAD Management/Service Quality Data). See table 2-13.106 page 2-13-89.

2-15.2.81 Magnetic Stripe Contents

Purpose: Contains Track 2 Data read from track 2 of the magnetic stripe, *excluding* Start Sentinel, End Sentinel and the LRC character.

Format: b19.

Contents: Data from track 2.

Remarks: Magnetic Stripe Contents is extracted from Track 2 Data. The Magnetic Stripe Contents is right justified and padded with 'F'. The last four bits will always have the value 'FF'.

2-15.2.82 Magstripe Indicator

Purpose: To indicate for the external kernel a number of conditions related to MSD transactions.

Format: b1 (1 byte).

Contents: The Magstripe Indicator is coded according to 2-15.16.

Remarks: The data element Magstripe Indicator is provided to the PSAM in the *Get Contactless AID related Information* command response.

Table 2-15.16 - Coding of the Magstripe Indicator

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	x	x	<u>MSD handling:</u>
-	-	-	-	-	-	0	0	- MSD not allowed
-	-	-	-	-	-	0	1	- MSD allowed
-	-	-	-	-	-	0	0	- MSD forced
-	-	-	-	-	-	0	1	- RFU
x	x	x	x	x	x	-	-	RFU

2-15.2.83 Maximum Deposit

Purpose: To indicate the maximum amount allowed to deposit for later charge of the card.

Format: b4 (4 bytes).

Contents: Amount is coded as an unsigned binary integer.

Remarks: The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units. The Maximum Deposit can be obtained from the response to the *Validate Data 2* command. If Maximum Deposit is absent from the host, all 4 bytes will be filled with 'F's.

2-15.2.84 MDOL (MAD-Handler Data Object List)

Purpose: To hold a list of data objects (tag and length) to be passed to the PSAM from the terminal. MDOL1 is returned in the response to the *Initiate Payment* command while MDOL2 is returned in the response to the *Payment* command.

Format: b, variable length.

Remarks: MDOL1 and MDOL2 will contain a list of data objects to be passed by the PSAM to the ICC (indicated in CDOL1 and CDOL2 respectively) that do not already reside in the PSAM. Candidates for the MDOL are the data elements which origin in the terminal.

2-15.2.85 MDOL Data

- Purpose:* To hold MDOL data contained in a MDOL.
- Format:* b, variable length.
- Remarks:* In MDOL Data, data from the MDOL are stored as concatenated data elements.

2-15.2.86 ME_{ADDRESS} (Merchant Address)

- Purpose:* To indicate the address (street name and number) for the merchant where the terminal is located.
- Format:* anps24 (24 bytes).
- Contents:* Characters coded according to ref. 12: "ISO/IEC 8859-15".
Trailing blanks are used for padding and may be removed before printing.
- Remarks:* The Merchant Address is printed on the cardholder receipt.

2-15.2.87 ME_{BRN} (Business Registration Number)

- Purpose:* To indicate the Business Registration Number for the merchant.
- Format:* anps12 (12 bytes).
- Contents:* Characters coded according to ref. 12: "ISO/IEC 8859-15".
Trailing blanks are used for padding and may be removed before printing.
- Remarks:* The Business Registration Number (e.g. in Denmark, CVR-Number) may be printed on the cardholder receipt.

2-15.2.88 ME_{CITY} (Merchant City Name)

- Purpose:* To indicate the city for the merchant where the terminal is located.
- Format:* anps 16 (16 bytes).
- Contents:* Characters coded according to ref. 12: "ISO/IEC 8859-15".
Trailing blanks are used for padding and may be removed before printing.
- Remarks:* The Merchant City Name is printed on the cardholder receipt.

2-15.2.89 ME_{NAME} (Merchant Name)

- Purpose:* To indicate the official name of the merchant where the terminal is located.
- Format:* anps18 (18 bytes).
- Contents:* Characters coded according to ref. 12: "ISO/IEC 8859-15".
Trailing blanks are used for padding and may be removed before printing.
- Remarks:* The Merchant Name is printed on the cardholder receipt.

2-15.2.90 ME_{NUMBER} (Merchant Number)

- Purpose:* To indicate the ID of the merchant where the terminal is located.
The Merchant Number is unique within a given Nets defined debit/credit application.
- Format:* n10 (5 bytes).
- Contents:* BCD coded.
- Remarks:* The Merchant Number is printed on the cardholder receipt.

2-15.2.91 ME_{PHONE} (Merchant Phone No.)

- Purpose:* To indicate the phone number of the merchant where the terminal is located (or a central helpdesk).
- Format:* anps24 (24 bytes).
- Contents:* Characters coded according to ref. 12: "ISO/IEC 8859-15".
Trailing blanks are used for padding and may be removed before printing.
- Remarks:* The Merchant Phone No. is printed on the cardholder receipt.

2-15.2.92 ME_{ZIP} (Merchant Postal Code)

- Purpose:* Indicates the postal code (ZIP code) for the merchant where the terminal is located.
- Format:* anps8 (8 bytes).
- Contents:* Characters coded according to ref. 12: "ISO/IEC 8859-15".
Trailing blanks are used for padding and may be removed before printing, e.g. if another data element (such as the merchant city) is printed on the same line.
- Remarks:* The Merchant Postal Code is printed on the cardholder receipt.

2-15.2.93 MI (Merchant Initiative)

- Purpose:* To indicate parameters forced by the merchant, e.g. if the cardholder has forgotten the PIN, the merchant may request a signature based transaction by setting Merchant Initiative to B'10000010. Furthermore, this data element indicates additional whether an online or offline connection is forced by the merchant. Depending on card scheme rules, the PSAM may reject this request(s).
- Format:* b1 (1 byte).
- Contents:* See table 2-15.17.

Table 2-15.17 - Coding of Merchant Initiative

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	<u>Forced CVM:</u>
0	-	-	-	-	-	-	-	- CVM handling is default, ignore b2–b1
1	-	-	-	-	-	-	-	- CVM handling is alternative/forced, see b2–b1
x	-	-	-	-	-	x	x	<u>Signature:</u>
1	-	-	-	-	-	1	0	- Signature forced to be used as CVM
x	-	-	-	-	-	x	x	<u>PIN:</u>
1	-	-	-	-	-	0	1	- PIN forced to be used as CVM
x	-	-	-	-	-	x	x	<u>Selectable Kernel Configurations:</u>
1	-	-	-	-	-	0	0	- Use alternative terminal configuration
-	x	-	-	-	-	-	-	<u>Forced/preferred Online/Offline:</u>
-	0	-	-	-	-	-	-	- Default Online/Offline, ignore b6–b5
-	1	-	-	-	-	-	-	- Forced/preferred Online/Offline, see b6–b5
-	x	x	x	-	-	-	-	<u>Offline:</u>
-	1	1	0	-	-	-	-	- Offline requested to be forced
-	x	x	x	-	-	-	-	<u>Online:</u>
-	1	0	1	-	-	-	-	- Online requested to be forced
-	x	x	x	-	-	-	-	<u>Preferred Offline:</u>
-	1	1	1	-	-	-	-	- Offline preferred but Online accepted
-	-	-	-	x	-	-	-	<u>Addendum Record:</u>
-	-	-	-	0	-	-	-	- Addendum Record(s) <i>not</i> to be attached
-	-	-	-	1	-	-	-	- Addendum Record(s) to be attached
-	-	-	-	-	x	-	-	<u>Overrule Amount Limits:</u>
-	-	-	-	-	0	-	-	- Amount limits effective
-	-	-	-	-	(1)	-	-	- Not allowed

Remarks: Conflicting values (e.g. PIN & Signature forced) will result in rejection. Choosing Selectable Kernel Configurations without loading an alternative configuration into the PSAM will result in a rejection. Forcing CVM (b8 = 1) and setting an illegal bit combination will result in a rejection. Forcing Online/Offline (b7 = 1) without setting any of the corresponding bits (b6 or b5) will result in a rejection.

Example: A forced Offline transactions (without forced CVM) has the value of '60'. The PSAM will select the appropriate CVM (with the highest priority).

2-15.2.94 Mode

Purpose: To indicate parameters applicable for the *Get Debit/Credit Properties* command with Identifier '000F'.

Format: b2 (2 bytes).

Contents: See table 2-15.18 and 2-15.19.

Table 2-15.18 - Byte 1 (MSB) of Mode

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	RFU

Table 2-15.19 - Byte 2 (LSB) of Mode

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	<u>Track2 Input Data:</u>
-	-	-	-	-	-	-	0	- Track2 Data in cleartext
-	-	-	-	-	-	-	1	- Track2 Data enciphered
-	-	-	-	-	-	x	-	<u>PIN Entry:</u>
-	-	-	-	-	-	0	-	- PIN Entry <i>not</i> requested
-	-	-	-	-	-	1	-	- PIN Entry requested
-	-	-	-	-	x	-	-	<u>Amount Confirmation:</u>
-	-	-	-	-	0	-	-	- Amount Confirmation <i>not</i> requested
-	-	-	-	-	1	-	-	- Amount Confirmation requested
x	x	x	x	x	-	-	-	RFU

2-15.2.95 MTI (Message Type Identifier)

Purpose: A four (4) digit field describing the version number, message class, message function and the transaction originator.

Format: an4 (4 bytes).

Contents: The following MTIs are used: 0106, 0107, 0116, 0126, 0127, 0136, 0206, 0207, 0216, 0226, 0227, 0236, 0360, 0370, 0426, 0427, 0436, 0624, 0625, 0634, 0804, 0805, 0814 and 0844.

2-15.2.96 MTI of the Original Message

Purpose: To identify messages with financial impact (for report purposes). The MTI of the Original Message (tag 'D2') can be found in the APACS header. Tag 'D2' is maintained by the PSAM.

Format: an4 (4 bytes)

Contents: TLV coded.

Remarks: If no original MTI is available, the current MTI will be indicated. Tag 'D2' will only appear together with tag 'D1' (Reference STAN)

2-15.2.97 PAN (Primary Account Number)

Purpose: To hold the Primary Account Number uniquely defining the cardholder's account at the card issuer.

Format: n..19 (up to 10 bytes).

Contents: BCD coded, with trailing a 'F' if the PAN consists of an odd number of digits.

Remarks: If the terminal supports Card Data Protection, the PAN returned in the command responses will be truncated according to the Card Scheme rules, i.e.

leaving the first 6 and last 4 digits unmasked. The remaining digits are replaced by 'A'. The full PAN is still padded with 'F' for byte boundary alignment if needed.

Example: 457160AAAAAA4625.

2-15.2.98 PAN Sequence Number

Purpose: Identifies and differentiates cards with the same PAN.

Format: n2 (1 byte).

Contents: BCD coded.

Remarks: The term "Card Sequence Number" is used in APACS messages, field 23.

2-15.2.99 PAN_{FROM}

Purpose: To specify the first PAN-prefix in the range covered by this MSC Selection Record.

Format: n8 (4 bytes).

Contents: BCD coded.

Remarks: The PAN_{FROM} value is included in the prefix range.

2-15.2.100 PAN_{TO}

Purpose: To specify the last PAN-prefix in the range covered by this MSC Selection Record.

Format: n8 (4 bytes).

Contents: BCD coded.

Remarks: The PAN_{TO} value is included in the range.

2-15.2.101 Payment Conditions

Purpose: To indicate additional information on a transaction type.

Format: an6 (6 bytes).

Contents: At the discretion of the issuer/merchant.

Remarks: None.

2-15.2.102 PCI Data

Purpose: To indicate to the host the extended configuration of the terminal, Payment Application and Cash Register. Makes it possible to perform a central trace of the status of the terminal.

Format: Binary, variable length. TLV encoded data as received from the terminal in the *Install 2* command. The PSAM will not validate the syntax or content.

Contents: TLV coded information on terminal parameters (see table 2-15.20).

Remarks: Data is identified with Tag 9C in Field 46 of an APACS Install message (see example below).

The data elements listed in Table 2-15.20 are applicable. Tag '9F97' and '9F98' correspond to Hardware Version Number (b2) and Software Version Number (b2), but here in a more descriptive representation.

Table 2-15.20 - PCI Data

Tag	Data element	Length (bytes)	Format	Mandatory/Conditional
'9F95'	PED SW version	Var.	b	C
'9F96'	PED HW version	Var.	b	C
'9F97'	Terminal HW platform	Var.	b	M
'9F98'	Terminal PA version	Var.	b	M
'9F99'	ECR IF name	Var.	b	C
'9F9A'	ECR SW version	Var.	b	C
'9F9B'	ECR PA version	Var.	b	C
'9F9C'	EMV checksum	8	b	M
Maximum length:		198 bytes		
Legend: Conditional (if the device/unit is present)				
Example: 3943 0024 9F97 0F 313233343536373839313132333435 9F98 04 31323334 9F9C 08 1C34259453443AB6				

2-15.2.103 PCT PAN_{FROM}

Purpose: To specify the first PAN-prefix in the range covered by the Processing Condition Table.

Format: n12 (6 bytes).

Contents: BCD coded.

Remarks: The PAN_{FROM} value is included in the prefix range. Found in the generic Processing Condition Table, table 1-10.5 page 1-10-28.

2-15.2.104 PCT PAN_{TO}

Purpose: To specify the last PAN-prefix in the range covered by the Processing Condition Table.

Format: n12 (6 bytes).

Contents: BCD coded.

Remarks: The PAN_{TO} value is included in the prefix range. Found in the generic Processing Condition Table, table 1-10.5 page 1-10-28.

2-15.2.105 PIN Block Format

Purpose: To indicate in the *Get Debit/Credit Properties* command (with Identifier = '000F') which PIN block format the issuer expect.

Format: b1 (1 byte).

Contents: See table 2-15.21.

Remarks: See also the data element Mode.

Table 2-15.21 - PIN Block Format

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	–	x	<u>Format 0 PIN block:</u>
–	–	–	–	–	–	–	0	– Format 0 PIN block <i>not</i> request
–	–	–	–	–	–	–	1	– Format 0 PIN block request
–	–	–	–	–	–	x	–	<u>Format 1 PIN block:</u>
–	–	–	–	–	–	0	–	– Format 1 PIN block <i>not</i> request
–	–	–	–	–	–	1	–	– Format 1 PIN block request
–	–	–	–	–	x	–	–	<u>Format 2 PIN block:</u>
–	–	–	–	–	0	–	–	– Format 2 PIN block <i>not</i> request
–	–	–	–	–	1	–	–	– Format 2 PIN block request
–	–	–	–	x	–	–	–	<u>Format 3 PIN block:</u>
–	–	–	–	0	–	–	–	– Format 3 PIN block <i>not</i> request
–	–	–	–	1	–	–	–	– Format 3 PIN block request
x	x	x	x	–	–	–	–	RFU
Legend: Only one bit must be set to B'1.								

2-15.2.106 PIN Data

Purpose: To hold PIN related data.

Format: LPKM_{pp} bytes.

Remarks: The data is encrypted under the PIN Pads public key.

2-15.2.107 POS Capability Code

Reference: Ref. 25: "APACS Standard 60".

Purpose: To indicate the capabilities of the terminal in which the transaction was created.

Format: an6.

Contents: See section 2-13.9.4 page 2-13-66.

Remarks: The POS Capability Code is transmitted in field 21 in APACS 60 messages.

2-15.2.108 POS Entry Mode

Reference: Ref. 25: "APACS Standard 60".

Purpose: To indicate the circumstances under which the transaction was created.

Format: n6 (3 bytes).

Contents: See section 2-13.9.5 page 2-13-70.

Remarks: The POS Entry Mode is transmitted in field 22 in APACS 60 messages.

2-15.2.109 PSAM Code Checksum

Purpose: To uniquely identify the PSAM code.

Format: b8 (8 bytes).

Contents: A checksum calculated on the EMV related part of the PSAM code.

Remarks: The PSAM Code Checksum shall be displayed/printed as 16 hexadecimal digits. This checksum is independent of the actual terminal configuration.

2-15.2.110 PSAM Config Checksum

- Purpose:* To uniquely identify the PSAM code and PSAM configuration.
- Format:* b8 (8 bytes).
- Contents:* A checksum calculated on both the EMV related part of the PSAM code and PSAM configuration. The following data elements are part of the checksum:
- Terminal Capabilities (3 bytes)
 - Additional Terminal Capabilities (5 bytes)
 - Terminal Type (1 byte)
 - PSAM Version (1 byte)
- Remarks:* The PSAM Config Checksum shall be displayed/printed as 16 hexadecimal digits. This checksum is identical for terminals with the same configuration.

2-15.2.111 PSAM D/C Life Cycle State

- Purpose:* Indicating the present state of the PSAM D/C Life Cycle.
- Format:* b1 (1 byte).
- Contents:* The following values are defined:
- '14': D/C key(s) loaded
 - '1C': Activation data loaded
 - 'F0': Blocked
- Remarks:* Life cycle states relevant for the terminal.

2-15.2.112 PSAM Parameters

- Purpose:* To transfer the current settings of the PSAM and the Terminal to the host. To be able to monitor the configuration from a central site.
- Format:* b14(14 byte).
- Contents:* Two data elements are returned:
- Tag 9F91 (4 bytes) The latest value for Terminal Settings received from the terminal preceded by 3 bytes 00 (RFU) to allow for future increase.
 - Tag 9F92 (10 bytes) The value of PSAM Settings (1 byte) followed by the value of Signature Settings (1 byte) followed by 8 bytes of (64) Miscellaneous Flags.
- Remarks:* The content is inserted by the PSAM as part of the Installation flow. Data is identified with Tag 9D in Field 46 of an APACS Install message.

2-15.2.113 PSAM Security Configuration

- Purpose:* To present the PSAM security setting to the Merchant.
- Format:* n b30 (30 byte blocks).
- Contents:* The security related information from the PSAM presented as ASCII text. The current content is:
- The PSAM ID as printed on the SIM card and the receipts.
 - The version of the PSAM, divided into;
 - major version number.minor version number.patch number;
 - The status of the following parameters:
 - LOG: 0 = syslog disabled,
1 = syslog enabled,
 - CDP: 0 = CDP disabled,
1 = CDP on response,

- 2 = CDP on command and response.
- PIN: 0 = PIN block format 2, PED RSA key exchange,
1 = PIN block format 1+or 2+, PED RSA key exchange,
2 = PIN block format 2, new PTS key exchange,
3 = PIN block format 1+ or 2+, new PTS key exchange.
- TA4: 0 = TAPA 46/47 command encrypted,
1 = TAPA 46/47 commands in clear text.
- EIE: 0 = No Extended Issuer Envelope,
1 = Extended Issuer Envelope supported.
- APE: 0 = APE and DAPE disabled, 1 = Only APE enabled,
2 = APE and DAPE enabled.
- CSH: 0 = Cash transactions not enabled,
2 = Cash transactions enabled, set for manual cash
3 = Cash transactions enabled, set for quasi-cash.
- PPU: 0 = Post purchase not enabled,
1 = Post purchase enabled.
- PRE: 0 = Post refund not enabled,
1 = Post refund enabled.
- DOM: 0 = Forced domestic transactions disabled,
1 = Forced domestic transactions enabled.

Remarks: This is informational data and should not be used for transaction purpose. There is at the present three lines of data but more may be added in the future.

A typical set of data could look like;
 PSAM:0000304728,VER:71.00.08
 LOG:1,CDP:1,PIN:0, TA4:0,EIE:0
 APE:0,CSH:0,PPU:0,PRE:0,DOM:0

2-15.2.114 PSAM Subversion

Purpose: Indicates the subversion number of the firmware present in the PSAM. Common for all applications in the PSAM.

Format: b1 (1 byte).

Contents: The PSAM subversion is coded as an unsigned binary integer.

Remarks: When changes are made in the source code, the PSAM Version will increase.

2-15.2.115 PSAM Version

Purpose: Indicates the version number of the firmware present in the PSAM.

Format: b1 (1 byte).

Contents: The PSAM Version is coded as an unsigned binary integer.

Remarks: When changes are made in the source code, the PSAM Version will increase. PSAM Version is indicated in the Historical Characters of the Answer-to-Reset.

2-15.2.116 PTS Request Data

Purpose: Transfer of information about the PTS key material to supply to the PSAM / PED.

Format: b33 (33 bytes).

Contents: Data needed by the host HSM to generate the key material to be used for secure transfer of data between the PSAM and the PED. See table 2-15.22 for details.

Remarks: The PTS Request Data is identified with Tag 9A in Field 46 of a APACS Install message. The detailed format depends on the value of element ALG_{PPSYNC}. The values shown are for the value '01'. So far, this is the only value defined.

Table 2-15.22 - PTS Request Data

Data element	Description	Length
ALG _{PPSYNC}	The algorithm identifier which implicitly defines the fixed format for tag 9A	1
ID _{PPCREATOR}	Identifier of the PED creator	4
ID _{PP}	Identifier of the PED	4
VK _{BDK,PED}	PED BDK Version Number	4
PED KEK Derivation Data		
VK _{PED}	Key Version	4
TS _{PED}	Time Stamp	4
VK _{BDK,PSAM}	PSAM BDK Version Number	4
PSAM KEK Derivation Data		
VK _{PSAM}	Key Version	4
TS _{PSAM}	Time Stamp	4
Total Length		33

2-15.2.117 PTS Response Data

Purpose: Transfer of key material to supply to the PSAM / PED.

Format: b74/51 (74/51 bytes).

Contents: Key information from the host to be used for secure transfer of data between the PSAM and the PED. See table 2-15.23 for details.

Remarks: The format of the response data depends on whether or not Master Key information is to be returned to the PSAM. The PTS Response Data is identified with Tag 9B in Field 46 of a APACS Install message. The detailed format depends on the value of element ALG_{PPSYNC}. The values shown are for ALG_{PPSYNC} = '01'. This is so far, this is the only value defined.

Table 2-15.23 - PTS Response Data

Data element	Description	Length
PED KEK Derivation Data VK _{PED} TS _{PED}	Key Version Time Stamp	4 4
[SDK] _I KEK_PED	The PED Session Derivation Key enciphered by the PED KEK (which must first be derived by the PED in case the PED KEK Derivation Data changed)	16
PSAM KEK Derivation Data VK _{PSAM} TS _{PSAM}	Key Version Time Stamp	4 4
[SDK] _I KEK_PSAM	The PSAM Session Derivation Key enciphered by the PSAM KEK (which must first be derived by the PSAM in case the PSAM KEK Derivation Data changed)	16
KCV _{SDK}	Key Check Value for PED/PSAM Session Derivation Key	3
[MK _{PSAM}] _{KEK} data	The PSAM Master Key enciphered by KEK-DATA	16 ¹⁾
VK _{BDK,PSAM}	PSAM BDK Version Number	4 ¹⁾
KCV _{MK_PSAM}	The Key Check Value for PSAM Master Key	3 ¹⁾
Total Length		74/51 ¹⁾
Legend:		
¹⁾ The size of the response data depends on whether or not PSAM Master key information is distributed in the response.		

2-15.2.118 Random_{NUMBER}

Purpose: To provide a true random number to be used by the terminal. Can be requested at any time.

Format: b (Variable).

Contents: Random number.

Remarks: The PSAM returns a random number with the length requested by the terminal. See 2-14.5.10 for additional information.

2-15.2.119 RECON_Counter_{ID}

Purpose: To inform the CAD of the ID of a reconciliation counter.

Format: n3 (2 bytes).

Contents: The ID number of the counter to print on reconciliation reports.

Remarks: BCD coded with a leading '0' as padding.

2-15.2.120 RECON_Counter_{NAME}

Purpose: To inform the CAD of the name of a reconciliation counter.

Format: ans16 (16 bytes).

Contents: The counter name to print on reconciliation reports.

Remarks: None.

2-15.2.121 RECON_PAN_{FROM}

Purpose: To specify the first PAN-prefix in the range covered by this RECON Counter Record.

Format: n12 (6 bytes).

Contents: BCD coded.

Remarks: The PAN_{FROM} value is included in the prefix range.

2-15.2.122 RECON_PAN_{TO}

Purpose: To specify the last PAN-prefix in the range covered by this RECON Counter Record.

Format: n12 (6 bytes).

Contents: BCD coded.

Remarks: The PAN_{TO} value is included in the range.

2-15.2.123 Reference STAN

Purpose: To indicate a link from an advice with financial impact (Financial Advice or Reversal Advice) to a specific Transaction Request. Reference STAN is the value of the data element STAN indicated in the response to the *Initiate Payment* command. The Reference STAN (tag 'D1') can be found in the APACS header.

Format: n6 (3 bytes).

Contents: Unique number.

Remarks: Tag 'D1' will only be included if the advice has financial impact, i.e. a Financial Advice or Reversal Advice where the original MTI was either 0206 or 0226.

2-15.2.124 RID_{PSAM}

Purpose: To make the identifier of a PSAM Creator unique.

Format: 5 bytes binary.

Contents: 'A0 00 00 01 20'.

Remarks: The identifier of the entity that assigns identifiers to certified PSAM Creators (ID_{PSAMCREATOR}), assigned as specified in ref. 9: "ISO/IEC 7816-5".

2-15.2.125 Salt

Purpose: Random data that are used as an additional input to a one-way function that hashes a PAN or PAN/Expiration Date.

Format: b32 (32 bytes).

Contents: Random data.

Remarks: The salt will always be encrypted at the interfaces.

NOTE: The size may change in the future if other Algorithms are used.

2-15.2.126 Salt Version

- Purpose:* Random data that are used as an additional input to a one-way function that hashes a PAN or PAN/Expiration Date.
- Format:* b1 (1 byte).
- Contents:* Serial number, incremented for each updated version.

2-15.2.127 Scheme Id

- Purpose:* A unique value identifying the Electronic Receipt Company (ERCo).
- Format:* b1 (1 byte).
- Contents:* At the discretion of Nets. In the range '01' – '20', see Table 2-15.24.
- Remarks:* Each Electronic Receipt Company will be assigned a unique Scheme Id by Nets.

Table 2-15.24 - Defined Scheme Id's

Value	ERCo (Electronic Receipt Company)
'01'	Kvittering.dk
'02'	eKvittering Aps
'03'..'1F'	To be defined
'20'	Nets Denmark A/S

2-15.2.128 Scheme Id Bitmap

- Purpose:* Bitmap that identifies the Electronic Receipt Companies supported by the terminal. The bitmap is able to support up to 32 different bitmaps.
- Format:* b4 (4 bytes).
- Contents:* Each bit indicates a Scheme Id. Least significant bit indicates Scheme Id no. '01', representation B '00000000 00000000 00000000 00000001'.

2-15.2.129 Seed

- Purpose:* To indicate the SALT version used for the hash computation for Electronic Receipts.
- Format:* b4 (4 bytes).
- Contents:* A 4 bytes pattern determined by the terminal.

2-15.2.130 Selectable Kernel Configurations

- Purpose:* A set of data elements specifying a Selectable Kernel Configurations setup of the terminal. Transferred to the PSAM in the *Set D/C Properties* (Id = '8003') command.
- Format:* b16 (16 bytes).
- Contents:* The Selectable Kernel Configuration of the terminal, formatted as in the command *Exchange Debit/Credit Static Information*.

Table 2-15.25 - Selectable Kernel Configurations - Data elements

Data elements	Size (bytes)
Terminal Capabilities	3
Additional Terminal Capabilities	5
Software Version Number ¹⁾	2
Hardware Version Number ¹⁾	2
Terminal Approval No. ¹⁾	2
MAD Handler ID ¹⁾	8
Terminal type	1
POS Capability Code	6
Info Level ¹⁾	1

Remarks: The elements marked with ¹⁾ shall be the same as used initially in the command *Exchange Debit/Credit Static Information*.

2-15.2.131 Service Code

Reference: Ref. 5: "ISO/IEC 7813".

Purpose: A three-digit code assigned by the ISO/IEC technical body.

Format: n3 (2 bytes).

Contents: See reference above.

Remarks: Padded with a leading zero.

2-15.2.132 Service Packs Supported

Purpose: Indicating the Service Packs supported by the PSAM.

Format: b1 (1 byte).

Contents: See table 2-15.26.

Remarks: Part of the Additional PSAM Info returned in the *Get Debit/Credit Properties* response. The data element "Terminal Approval No." indicates which Service Packs the terminal supports.

Table 2-15.26 - Coding of Service Packs Supported

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	x	x	<u>Service Packs Supported:</u>
0	0	0	0	0	0	0	0	- Baseline (No Service Pack supported)
-	-	-	-	-	-	-	1	- Service Pack No. 1 supported
-	-	-	-	-	-	1	-	- Service Pack No. 2 supported
-	-	-	-	-	1	-	-	- RFU (Service Pack No. 3 supported)
x	x	x	x	x	-	-	-	- RFU

2-15.2.133 Settings_{CL}

Purpose: To hold information concerning a specific AID.

Format: b4 (4 bytes).

Contents: See table 2-15.27.

Remarks: Bits b9 - b32 are RFU

Table 2-15.27 - Coding of Settings_{CL}

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	–	x	<u>Contactless technology (ICC):</u>
–	–	–	–	–	–	–	0	– ICC not supported
–	–	–	–	–	–	–	1	– ICC supported
–	–	–	–	–	x	x	–	<u>Contactless technology (MSD):</u>
–	–	–	–	–	0	0	–	– MSD not supported
–	–	–	–	–	0	1	–	– MSD supported
–	–	–	–	–	1	0	–	– MSD forced
–	–	–	–	–	1	1	–	– RFU
–	–	–	–	x	–	–	–	<u>Partial/full match on AID:</u>
–	–	–	–	0	–	–	–	– Partial match
–	–	–	–	1	–	–	–	– Full match
–	–	–	x	–	–	–	–	<u>Status Check:</u>
–	–	–	0	–	–	–	–	– Not supported
–	–	–	1	–	–	–	–	– Supported
–	–	x	–	–	–	–	–	<u>Zero Amount:</u>
–	–	0	–	–	–	–	–	– Not allowed
–	–	1	–	–	–	–	–	– Allowed
x	x	–	–	–	–	–	–	RFU

2-15.2.134 Signature Verification

Purpose: To indicate whether signature verification by the merchant is required or not.

Format: b1 (1 byte).

Contents: See table 2-15.28.

Remarks: Part of the response to *Exchange Debit/Credit Static information* command.

Table 2-15.28 - Coding of Signature Verification

Value	Meaning
'00'	Signature verification is not required
'FF'	Signature verification is required
'01'..'FE'	RFU

2-15.2.135 Software Version Number

Purpose: To indicate the version number of the MAD-Handler application.

Format: b2 (2 bytes).

Contents: At the discretion of the Terminal Supplier. A new software version should, however, have an increased version number.

2-15.2.136 STAN (System Trace Audit Number)

Purpose: A number assigned by a transaction originator to assist in identifying a transaction uniquely.

Format: n6 (3 bytes).

Contents: Unique number generated by the PSAM.

2-15.2.137 Statistics

- Purpose:* To hold statistical data of the behavior of the terminal.
- Format:* Binary, variable length up to 48 bytes.
- Contents:* TLV coded according to section 2-13.9.11 page 2-13-87.
- Remarks:* The following tags are candidates: 'TD', 'TE', 'TF', 'TG' and 'TH'. Note that the 48 bytes are the maximum amount of data that the PSAM can handle. If each of the above mentioned tags appear once the total length is 42 bytes.

2-15.2.138 Stop List Status

- Purpose:* To indicate the result of a search in the Stop List.
- Format:* b1 (1 byte).
- Contents:* See table 2-15.29.

Table 2-15.29 - Coding of Stop List Status

Value	Meaning
'00'	Card not found in Stop List
'01'	Card found in Stop List
'02'	Card found in Stop List (pick-up requested)
'03'	Stop List not found
'04'..'7F'	RFU
'80'	Voice Authorization rejected
'81'..'FF'	RFU

2-15.2.139 SUBVERSION_{PCT}

- Purpose:* To indicate the subversion number of the Processing Condition Table.
- Format:* b1 (1 byte).
- Contents:* The SUBVERSION_{PCT} is coded as an unsigned binary integer.
- Remarks:* When minor changes are made in the Processing Condition Table, the SUBVERSION_{PCT} will increase. Found in the generic Processing Condition Table, table 1-10.5 page 1-10-28.

2-15.2.140 TAG_{AdditionalInfo}

- Purpose:* To indicate the type of Additional Information inside the Issuer Envelope Data.
- Format:* anps2 (2 bytes).
- Contents:* DCC: ZW ('5A57')
OPEL: Z0 ('5A30')
SE: TZ ('545A')

2-15.2.141 Terminal Approval No.

- Purpose:* To uniquely identify a certified terminal.
- Format:* b2 (2 bytes).
- Contents:* A unique terminal identifier assigned by Nets, in the format shown in table 2-15.30 and 2-15.31.

Table 2-15.30 - Most Significant Byte of the Terminal Approval No.

b16	b15	b14	b13	b12	b11	b10	b9	Meaning
x	x	x	–	–	–	–	–	<u>Service Pack No.:</u>
0	0	0	–	–	–	–	–	– No Service Pack requested
0	0	1	–	–	–	–	–	– Service Pack No. 1 requested
0	1	0	–	–	–	–	–	– Service Pack No. 2 requested
x	x	x	–	–	–	–	–	– RFU
–	–	–	x	x	x	x	x	<u>Terminal Manufacturer ID as assigned by Nets</u>

Table 2-15.31 - Least Significant Byte of the Terminal Approval No.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	–	–	–	–	<u>Terminal Category:</u>
0	0	0	0	–	–	–	–	– RFU
0	0	0	1	–	–	–	–	– Attended
0	0	1	0	–	–	–	–	– RFU
x	0	1	1	–	–	–	–	– Unattended (UPT)
x	x	x	x	–	–	–	–	– RFU
–	–	–	–	x	x	x	x	<u>Serial Number</u>

2-15.2.142 Terminal Checksum

- Purpose:* To uniquely identify the part of the EMV level 2 kernel residing in the terminal.
- Format:* b, variable (up to 200 bytes).
- Contents:* Concatenation of different data elements identifying the terminal application.
- Remarks:* Shall at least include an EMV kernel checksum (4-20 bytes) and one or more Transaction Type(s) applicable for the terminal.

2-15.2.143 Terminal Contactless Floor Limit

- Purpose:* Indicates the limit for which contactless transactions can be conducted in the Terminal relating to the AID.
- Format:* n12 (6 bytes).
- Contents:*
- Remarks:* See ref. 21: "Entry Point Specification" for further information.

2-15.2.144 Terminal Contactless Transaction Limit

- Purpose:* Indicates the maximum transaction amount relating to the AID.
- Format:* n12 (6 bytes).
- Contents:*
- Remarks:* See ref. 21: "Entry Point Specification" for further information.

2-15.2.145 Terminal CVM Required Limit

- Purpose:* Indicates the contactless floor limit in the Terminal relating to the AID.
- Format:* n12 (6 bytes).
- Contents:*
- Remarks:* See ref. 21: "Entry Point Specification" for further information.

2-15.2.146 Terminal Decision Flags

Purpose: To indicate conditions that may influence the way of performing the transactions when using an Entry Point. These flags are handled and maintained by the terminal.

Format: b1 (1 byte).

Contents: See table 2-15.32.

Remarks: Related to the Entry Point handling. The unused bits (RFU) shall be set to zero.

Table 2-15.32 - Terminal Decision Flags

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	<u>Terminal Contactless Transaction Limit:</u>
-	-	-	-	-	-	-	0	- Not exceeded
-	-	-	-	-	-	-	1	- Exceeded
-	-	-	-	-	-	x	-	<u>Terminal Contactless Floor Limit:</u>
-	-	-	-	-	-	0	-	- Not exceeded
-	-	-	-	-	-	1	-	- Exceeded
-	-	-	-	-	x	-	-	<u>Terminal CVM Required Limit:</u>
-	-	-	-	-	0	-	-	- Not exceeded
-	-	-	-	-	1	-	-	- Exceeded
-	-	-	-	x	-	-	-	<u>Status Check Requested:</u>
-	-	-	-	0	-	-	-	- Status Check <i>not</i> Requested
-	-	-	-	1	-	-	-	- Status Check Requested
-	-	-	x	-	-	-	-	<u>Zero Amount:</u>
-	-	-	0	-	-	-	-	- Not Zero Amount
-	-	-	1	-	-	-	-	- Zero Amount
-	-	x	-	-	-	-	-	<u>Contactless Application:</u>
-	-	0	-	-	-	-	-	- Allowed
-	-	1	-	-	-	-	-	- Not allowed
x	x	-	-	-	-	-	-	RFU

2-15.2.147 Terminal Identification

Purpose: Designates the unique location of a terminal at a merchant.

Format: an8 (8 bytes).

Contents: At the discretion of the terminal vendor.

Remarks: It is important that the format of the Terminal Identification is correct. If not, the PSAM will reject transactions. An EMV defined data element identified by the tag '9F1C'.

2-15.2.148 Terminal Manufacturer ID

Purpose: To uniquely identify a Terminal Manufacturer.

Format: ans3.

Contents: At the discretion of Nets.

Remarks: Part of the MAD-Handler ID. See table 2-13.106 page 2-13-89.

2-15.2.149 Terminal Serial Number

Purpose: To uniquely identify a terminal under a specific Terminal Manufacturer.

Format: ans5.

Contents: At the discretion of Nets.

Remarks: Part of the MAD-Handler ID. See table 2-13.106 page 2-13-89.

2-15.2.150 Terminal Settings

Purpose: Defines the requested behavior of the terminal/PSAM during a transaction.

Format: b1 (1 byte).

Contents: See table 2-15.33.

Remarks: Terminal Settings are conveyed to the PSAM using the *Set Debit/Credit Properties* command with the Identifier equal '8001'. Please note that requested options may not always be supported.

Table 2-15.33 - Terminal Settings

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	<u>Entry handling:</u>
-	-	-	-	-	-	-	0	- Single-entry requested
-	-	-	-	-	-	-	1	- Multi-entry requested
-	-	-	-	-	x	x	-	<u>Card Data Protection (CDP):</u>
-	-	-	-	-	0	0	-	- CDP <i>not</i> active
-	-	-	-	-	0	1	-	- CDP active (responses enciphered)
-	-	-	-	-	1	0	-	- CDP active (resp./cmd. enciphered)
-	-	-	-	-	1	1	-	- RFU
-	-	-	-	x	-	-	-	<u>PIN block format:</u>
-	-	-	-	0	-	-	-	- According to ref.: 27 "TAPA, ver. 2.1"
-	-	-	-	1	-	-	-	- According to ref.: xx "TAPA, ver. 3.0"
-	-	-	x	-	-	-	-	<u>TAPA commands 46/47, clear text response:</u>
-	-	-	0	-	-	-	-	- TAPA 46/47 enciphered resp. if CDP
-	-	-	1	-	-	-	-	- TAPA 46/47 clear text resp. if CDP
-	-	x	-	-	-	-	-	<u>Logging information:</u>
-	-	0	-	-	-	-	-	- No logging information generated
-	-	1	-	-	-	-	-	- Logging information generated
-	x	-	-	-	-	-	-	<u>PIN Pad/PSAM Key Synchronization:</u>
-	0	-	-	-	-	-	-	- Old synchronization method used
-	1	-	-	-	-	-	-	- New synchronization method used
x	-	-	-	-	-	-	-	<u>Extended Issuer Envelope:</u>
0	-	-	-	-	-	-	-	- Extended Issuer Envelope <i>not</i> used
1	-	-	-	-	-	-	-	- Extended Issuer Envelope used

2-15.2.151 Token

Purpose: To hold data that uniquely identify a consumer card and related Authorization Request.

Format: b, variable length.

Contents: Unique consumer card and transaction data, see section 2-4.3 page 2-4-3, Tokens.

2-15.2.152 [Track Data]

- Purpose:* To hold enciphered track data read on an MSC. The Track Data listed below are enciphered by the KSES_{CDP} key.
- Format:* Variable, up to 64 bytes.
- Contents:* Random Number (4 bytes) || Track2/Track3 (up to 52 bytes) || Padding
- Remarks:* This data element is applicable when Card Data Protection is supported and a MSC transaction is performed.
Padding according to ref. 15: "ISO/IEC 9797", Padding method 2.

2-15.2.153 Track1 Data

- Purpose:* To hold track 1 data read from an MSC.
- Format:* Variable, up to 76 / 79 bytes.
- Contents:* Card data coded according to ref. 5: "ISO/IEC 7813".
- Remarks:* Two formats exists. In the one format digits are coded as 6 bit modified ASCII with separator(s) coded as hexadecimal '3E'. These characters constitute the entire track 1 with the exception of the start sentinel, the end sentinel and the LRC character.
In the other format data are supplied as full ASCII text. The characters constitute the entire track 1 including start sentinel, end sentinel and LRC.
- Example:* The text string %B45^ABC?* is in packet format encoded as '22', '14', '15', '3E', '21', '22', '23'. The string is in full ASCII format encoded as '25', '42', '34', '35', '5E', '41', '42', '43', '3F'.

2-15.2.154 Track2 Data

- Purpose:* To hold track 2 data read from an MSC.
- Format:* Variable, up to 19 bytes long.
- Contents:* Card data coded according to ref. 5: "ISO/IEC 7813".
- Remarks:* Digits are coded in BCD while separator(s) is coded as hexadecimal 'D'. Trailing 'F' is used as padding. These characters constitute the entire track 2 with the exception of the start sentinel, the end sentinel and the LRC character.
- Example:* The ASCII representation: 1234=5678?* is encoded as '12', '34', 'D5', '67', '8F'.

2-15.2.155 Track3 Data

- Purpose:* To hold track 3 data read from an MSC.
- Format:* 52 bytes.
- Contents:* Card data coded according to ref. 5: "ISO 4909".
- Remarks:* Digits are coded in BCD while separator(s) is coded as hexadecimal 'D'. Trailing 'F' is used as padding. These characters constitute the entire track 3 with the exception of the start and the end sentinel and the LRC character.
- Example:* The ASCII representation: 1234=5678?* is encoded as '12', '34', 'D5', '67', '8F'.

2-15.2.156 Transaction Category Code

- Purpose:* Used in Card Risk Management by MasterCard applications.
- Format:* b1 (1 byte).
- Contents:* A character coded according to ref. 12: "ISO/IEC 8859-15".
- Remarks:* This is a MasterCard specific data element. Ref. 31: "Terminal Requirements for Debit and Credit on Chip.". Tag '9F53'. Not carried in the clearing

data and should therefore not be used in the AC. Relation to Merchant Category Code.

2-15.2.157 Transaction Gratuity Amount

- Purpose:** To hold the gratuity amount.
- Format:** b4 (4 bytes).
- Contents:** Transaction Gratuity Amount is coded as an unsigned integer.
- Remarks:** The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units.

2-15.2.158 Transaction Identifier (TI)

- Purpose:** To prevent replay attacks for contactless transactions, e.g. by replacing a command with previously issued commands.
- Format:** b4 (4 bytes).
- Contents:** Random Number.
- Remarks:** Generated by the terminal for the *Initiate Contactless Payment* command. If rejected/declined by the terminal, the value shall be set to all zeroes in the *Complete Contactless Payment* command. The terminal shall never generate a Transaction Identifier equal to all zeroes in the *Initiate Contactless Payment* command.

2-15.2.159 Transaction Request (TR)

- Purpose:** To indicate to the PSAM which transaction type should be initiated.
- Format:** b1 (1 byte).
- Contents:** See table 2-15.34.

Table 2-15.34 - Coding of Transaction Request

Value	Meaning
'00'	Purchase
'01'	Refund
'02'	Original Authorization
'03'	Supplementary Authorization
'04'	Capture
'05'	Reversal (Authorization)
'06'	Cancellation
'07'	Extended Authorization
'08'	Top up (Contactless)
'09'	Extended Authorization 2
'0A'	Post Purchase
'0B'	Post Refund
'0C'..'FF'	RFU

2-15.2.160 Transaction Options (TO)

Purpose: To indicate specific options related to the contactless transactions.

Format: b1 (1 byte).

Contents: See table 2-15.35.

Table 2-15.35 - Coding of Transaction Options

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	–	x	<u>Issuer Envelope/Extended Issuer Envelope:</u>
0	–	–	–	–	–	–	0	– Issuer Envelope <i>not</i> to be attached
1	–	–	–	–	–	–	1	– Issuer Envelope to be attached
x	x	x	x	x	x	x	–	<u>Reserved for future use (RFU):</u>

2-15.2.161 Transaction State Information

Purpose: To indicate the transaction progress to the Merchant Application.

Format: b1 (1 byte).

Contents: See table 2-15.36 below.

Table 2-15.36 - Coding of Transaction State Information

Value	Meaning
'00'	Waiting for card
'01'	Waiting for application selection
'02'	Waiting for card validation
'03'	Waiting for amount
'04'	Waiting for PIN
'05'	Waiting for PIN and amount
'06'	Waiting (processing)
'07'	Waiting for online response
'08'..'1F'	RFU
'20'..'FF'	For proprietary use

2-15.2.162 Transaction Status

Purpose: To indicate to the PSAM the status of a transaction as seen from the terminal side.

Format: b1 (1 byte).

Contents: See table 2-15.37.

Table 2-15.37 - Coding of Transaction Status

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	–	–	–	–	–	–	–	<u>General Status:</u>
0	–	–	–	–	–	–	–	– Approved
1	–	–	–	–	–	–	–	– Declined
–	x	–	–	–	–	–	–	<u>Type of Complete Payment:</u>
–	0	–	–	–	–	–	–	– Complete Payment
–	1	–	–	–	–	–	–	– Delayed Complete Payment
x	–	x	x	x	x	x	x	<u>Additional information:</u>
0	–	0	0	0	0	0	0	– Successful
0	–	0	0	0	0	0	1	– Signature accepted
0	–	–	–	–	–	–	–	– RFU
0	–	1	1	1	1	1	1	– RFU
1	–	0	0	0	0	0	0	– Transaction aborted
1	–	0	0	0	0	0	1	– Signature rejected
1	–	0	0	0	0	1	0	– Goods or services not delivered
1	–	–	–	–	–	–	–	– RFU
1	–	1	1	1	1	1	1	– RFU

2-15.2.163 Transaction Total Amount

Purpose: To indicate the sum of Amount and Transaction Gratuity Amount.

Format: b4. Binary.

Contents: Transaction Total Amount is coded as an unsigned integer.

Remarks: The Amount sent to the acquirer for settlement of one transaction. See data element 2-15.2.11 page 2-15-4, Amount. The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units.

2-15.2.164 Transaction Type (TT)

Purpose: To indicate the type of transaction according to ref. 20: "EMV ICC Specification".

Format: n2 (1 byte).

Contents: '00' = Goods and services
 '01' = Cash
 '09' = Goods and services with cash disbursement
 '11' = Quasi-Cash and scrip
 '20' = Returns/Refunds

2-15.2.165 Truncated PAN

Purpose: To protect sensitive information by masking some of the digits in the PAN, see 2-15.2.97 for more information.

2-15.2.166 TS_{PED} KEK

Purpose: A timestamp to be used for key derivation data for the PED KEK. The time stamp can be used by the Host to determine whether PED KEK should be replaced.

Format: b4 (4bytes).

Remarks: The timestamp is "coded as a date in the format YYYYMMDD. For a PED KEK generated on October 17th 2012, the value is: ``20121017". The PED may validate this data element to prevent replay attacks.

2-15.2.167 TS_{PSAM} KEK

Purpose: A timestamp to be used for key derivation data for the PSAM KEK. The time stamp can be used by the Host to determine whether PSAM KEK should be replaced.

Format: b4 (4bytes).

Remarks: The timestamp is "coded as a date in the format YYYYMMDD. For a PSAM KEK generated on October 18th 2012, the value is: ``20121018". The PSAM may validate this data element to prevent replay attacks.

2-15.2.168 Type of Application

Purpose: Display text to be displayed on the Merchant Display (attended) or at the Cardholder Display (unattended) after power-on of the PSAM. The text is linked directly to the ID_{PSAMAPP}.

Format: an20.

Contents: ID_{PSAMAPP} = '8111': "Nets Debet/Kredit".

Remarks: If more than one application is supported, the display may alter between the texts.

2-15.2.169 Update Data

Purpose: To hold PSAM update data.

Format: LEN_{UPD} bytes. The format is tag specific.

Contents: The content of Update Data is identified by tag.

2-15.2.170 Update Number

Purpose: To indicate the segment number of a PSAM update and the total number of segments in the update.

Format: b1 (1 byte).

Contents: bit 8 - bit 5 Segment number of the update
bit 4 - bit 1 Total number of segments in the update

2-15.2.171 VAT Amount

Purpose: To transfer the VAT amount to the issuer.

Format: n10 (5 bytes).

Contents: VAT amount as printed on the receipt, value as calculated by the terminal, key entered by the merchant, or received from the ECR.

2-15.2.172 VERSION_{PCT}

Purpose: To indicate the version number of the Processing Condition Table.

Format: b2 (2 bytes).

Contents: The VERSION_{PCT} is coded as an unsigned binary integer.

Remarks: When changes that have impact on the size of the table are made in the Processing Condition Table, the VERSION_{PCT} will increase.

2-15.2.173 VK_{BDK}(Base Derivation Key Version)

Purpose: A reference to the <device> BDk that was used to derive the <device> MK. This value is transmitted together with the <device> Creator ID to the host in Installation Request messages..

Format: n8 (4 bytes).

Contents: A reference to the <device> BDk that was used to derive the <device> MK.

Remarks: This value is transmitted together with the <device> Creator ID to the host in Installation Request messages.

2-15.2.174 VK_{PED KEK}(KEK Version, PED)

Purpose: To be used for key derivation data for the PED KEK.

Format: b4 (4 bytes).

Remarks: The first value to assign is '00 00 00 01'. It is incremented for every new key generated. The PED must validate this data element to prevent replay attacks.

2-15.2.175 VK_{PSAM KEK}(KEK Version, PSAM)

Purpose: To be used for key derivation data for the PSAM KEK.

Format: b4 (4 bytes).

Remarks: The first value to assign is '00 00 00 01'. It is incremented for every new key generated. The PSAM must validate this data element to prevent replay attacks.

2-15.3 Data Elements specific to the Local PIN Application

2-15.3.1 Key Check Value (KCV)

- Purpose:* To verify the status of the LP-KEK or LP-Key shared between the Local PIN host and PSAM.
- Format:* b3 (3 bytes).
- Contents:* The 3 most significant bytes of the result of a triple-DES encryption of an 8-byte block of binary zeros.

2-15.3.2 Last PIN incorrect

- Purpose:* To indicate for the PSAM (PIN Pad) if the previous PIN entry for this card was incorrect. The Cardholder Display will display the text "Incorrect PIN".
- Format:* b1 (1 byte).
- Contents:* '00' - '0E' = Number of PIN tries left
'0F' = No information available
- Remarks:* The initial value of "Number of PIN tries left" may be provided by the local PIN host. Then it is up to the terminal to decrement the number for each incorrect PIN.

2-15.3.3 LP-KEK

- Purpose:* LP-KEK is the master key used for exchange of LP-Key.
- Format:* b16 (16 bytes).
- Contents:* Key value.
- Remarks:* The parity of the key is *not* validated by the PSAM.

2-15.3.4 LP-KEK-Version

- Purpose:* To indicate the version of the Key Exchange Key (KEK).
- Format:* b1 (1 byte).
- Contents:* '00' - 'FF'.

2-15.3.5 LP-Key

- Purpose:* Actual key used to encipher the plaintext PIN block.
- Format:* b16 (16 bytes).
- Contents:* Key value.
- Remarks:* The parity of the key is *not* validated by the PSAM.

2-15.3.6 LP-Key-Chain

Purpose: To indicate which key chain to be used when loading keys or when performing Local PIN Validation. Four key chains are defined.

Format: 1b (1 byte).

Contents: '00' = Key chain 0
'01' = Key chain 1
'02' = Key chain 2
'03' = Key chain 3
'04' - 'FF' = Reserved for future use.

2-15.3.7 LP-Key-Version

Purpose: To indicate the version of the LP-Key.

Format: b1 (1 byte).

Contents: '00' - 'FF'.

2-15.3.8 Maximum PIN digits

Purpose: To indicate the maximum number of PIN digits that is allowed for the local PIN application.

Format: b1 (1 byte).

Contents: '04' - '0C'.

2-15.3.9 Method Number

Purpose: To indicate in the *Load LP Keys* and *Local PIN Validation* commands whether plaintext or enciphered PIN is utilized.

Format: b1 (1 byte).

Contents: '00' = Plaintext PIN
'01' = Enciphered PIN
'02' - 'FF' = Reserved for future use.

Remarks: Note that for the *Load LP Keys* command, only Method Number = '01' (Enciphered PIN) is applicable.

2-15.3.10 Minimum PIN digits

Purpose: To indicate the minimum number of PIN digits that is allowed for the local PIN application.

Format: b1 (1 byte).

Contents: '04' - '0C'

2-15.3.11 Number of PIN tries left

Purpose: Used by the terminal to indicate for the PSAM the number of PIN tries left for this card. Except for the value '0F', the number will be shown transparently on the Cardholder Display.

Format: b1 (1 byte).

Contents: '00' - '0E' = Number of PIN tries left
'0F' = No information available

Remarks: The initial value of "Number of PIN tries left" may be provided by the local PIN host. Then it is up to the terminal to decrement the number for each incorrect PIN.

2-15.3.12 Time

- Purpose:* To specify a time-out value.
- Format:* b4 (4 bytes).
- Contents:* The time-out value in milliseconds.
- Remarks:* Time indicates the maximum time after which either data or an error response must be returned.

2-15.3.13 Timer Flag

- Purpose:* To indicate that a time-out value is specified.
- Format:* b1 (1 byte).
- Contents:* '00' = the message is not timed.
'80' = the message is timed.

2-15.3.14 Transaction Counter

- Purpose:* To indicate for the PSAM whether the transaction counter shall be incremented and a validation of the value shall be performed or not. The Transaction Counter is maintained by the PSAM. The Transaction Counter is used to encounter replay attacks.
- Format:* b4 (4 bytes).
- Contents:* Transaction Counter = '00 00 00 00' (No verification and *no* incrementation of the transaction counter).
Transaction Counter □ '00 00 00 00' (Verification and incrementation of the transaction counter).
- Remarks:* If the gap between the Transaction Counter value given in the *Local PIN Validation* command and the actual value is higher than 14, the transaction will be rejected and no incrementation will take place. If the gap between 1 to 14, the transaction counter will be incremented. Initial value of the PSAM transaction counter is zero.

Index, Book 2

Page references in **bold** type refer to either figures or tables.

A

- AAC, 2-13-90
- Accelerated PIN Entry, 2-5-29
- Accelerated PIN Entry Vs. Original Flow, **2-5-30**
- Access to the inside of the terminal, 2-7-5
- Account Type, 2-5-24, 2-5-46, **2-15-2**
 - Check/debit account, 2-13-66
 - Credit account, 2-13-66
 - Default account - unspecified, 2-13-66
 - Definition, 2-15-2
 - Savings account, 2-13-66
- Accuracy, Real time clock, 2-6-3
- Accurate Amount, 2-15-5
 - Get Amount 3, 2-14-116
- Acquirer Identifier, 2-5-28
- Action Code, 2-5-19, 2-5-91, 2-5-105, 2-5-114, 2-5-122
 - Applicable values, **2-13-83**
 - Definition, 2-15-2
 - Exception Handling, 2-5-124
 - Field 39, 2-13-82
 - National Use, **2-5-125**
 - Position 1, 2-5-124, **2-13-82**
 - Position 2, **2-13-82**
- Action Indicator, Definition, 2-15-3
- Add Addendum Record
 - Command, 2-5-87, 2-5-88
 - Description, 2-14-26
- Addendum, 2-15-6
- Addendum Record, 2-5-88, 2-13-55, 2-13-80, 2-14-26
 - Command flow, **2-5-90**
 - Definition, 2-15-3
 - Description, 2-5-87
 - Field 72, 2-13-94
- Addendum Status, 2-5-88, 2-14-26
- Additional AID Info, Get Debit/Credit Properties, 2-14-31
- Additional Data - National, Field 47, 2-13-89
- Additional Data Capture, 2-13-91
- Additional Info, 2-14-29, 2-14-41
- Additional MSC Info, Get Debit/Credit Properties, 2-14-31, 2-14-32
- Additional PSAM Info, 2-15-36
 - Get Debit/Credit Properties, 2-14-31
- Additional Response Data, Field 44, 2-13-86
- Additional Terminal Capabilities, 2-5-28, 2-5-93, 2-14-18, 2-14-20, 2-14-22
 - Field 46, 2-13-87
- Adjustment, 2-13-65
- Administrative Advice, Definition, **2-13-55**
- Administrative Transactions, **2-5-91**
 - Description, 2-5-91
- Advice Handling, **2-5-104**
- Advice Transfer, **2-5-91**, 2-5-105, **2-5-110**
 - Definition, 2-13-60
 - Description, 2-5-101, 2-5-104
- Advice Window Size
 - APACS Header, 2-13-6
 - Coding, 2-13-15
 - Description, 2-5-107
- Advice Window Size (Examples), **2-5-109**
- AID, 2-5-23, 2-13-90, 2-14-55, 2-14-84
 - Definition, 2-15-3
 - Exact match, 2-15-5
 - Get Debit/Credit Properties, 2-14-31, 2-14-32
 - Partial match, 2-15-5
- AIDEMV, 2-14-118
- AIP, 2-13-90
- Airlines, 2-13-81, 2-13-94
- ALG, Card Data Protection, 2-14-128
- Algorithm Id, 2-15-4
- ALGPPSYNC, 2-14-22
- ALGVLP, Definition, 2-15-4

- ALGVPPSYNC, 2-15-4
- Alpha-characters, 2-4-10, 2-6-6
- Alternative Kernel Configuration, **2-15-36**
- Amount, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-89, 2-14-118
 - Definition, 2-15-4
 - Get Debit/Credit Properties, 2-14-31
 - Local PIN, 2-14-124, 2-14-126
- Amount Authorized, Field 55, 2-13-90
- Amount Confirm Indicator, 2-5-126
- Amount Other, Get Amount 3, 2-14-116
- Amount Request
 - Definition, 2-15-5
 - Get Amount 3, 2-14-115
 - Service Pack No. 2, 2-8-5
- Amount Status
 - Definition, 2-15-5
 - Get Amount 3, 2-14-116
 - Service Pack No. 2, 2-8-5
- Amount, Other, 2-5-20, 2-5-73
 - Definition, 2-15-4
 - Field 55, 2-13-90
- Answer-to-Reset, 2-15-31
- AOSA, 2-15-6
- APACS, 2-5-117, 2-5-124, 2-13-6, 2-15-29
 - Example, **2-13-11**
- APACS Header, **2-13-6, 2-13-8**
- APACS MAC Key Version
 - APACS Header, 2-13-6
 - Coding, 2-13-14
- APACS Message Header, Description, 2-13-5
- APACS Message Types, **2-13-4**
- APACS60, 2-13-2
- APDU, 2-5-94, 2-14-4
- APE, Accelerated PIN Entry, 2-5-29
- Application Cryptogram, Field 55, 2-13-90
- Application Effective Date, 2-5-25
- Application Expiration Date, Field 55, 2-13-90
- Application Identifier
 - Definition, 2-15-3
 - Field 55, 2-13-90
- Application Initialization, 2-5-1
- Application Interchange Profile, Field 55, 2-13-90
- Application Label, Definition, 2-15-5
- Application layer, **2-13-2**
- Application Layers, 2-13-3
- Application Selection, 2-3-8
 - Introduction, **2-3-8**
- Application Selection Indicator, Definition, 2-15-5
- Application Status Words, 2-5-17, 2-14-4, 2-14-131
 - Exception Handling, 2-5-122
 - Field 46, 2-13-88
- Application Transaction Counter, Field 55, 2-13-90
- Approval Code, 2-5-21, 2-5-22
 - Definition, 2-15-5
 - Service Packs, 2-8-4
- Approval tone, 2-6-6
- ARQC, 2-13-90
- ASI
 - Commands, 2-14-37
 - Definition, 2-15-5
 - Get Debit/Credit Properties, 2-14-31
- ASN.1, 2-13-5
- ASW1 ASW2, 2-5-115, 2-5-124
 - Approved/Successful, **2-14-136**
 - Approved/Successful - Action Requested, **2-14-136**
 - Contactless - Technical failure, 2-14-151
 - Converted to Message Codes, **2-14-133**
 - Declined, **2-14-146**
 - Declined - Pick up, **2-14-149**
 - Error - Action Requested, **2-14-141**
 - Failed - No Retry, **2-14-151**
 - Failed - Retry, **2-14-149**
 - Range, **2-14-134, 2-14-135**
 - TAPA defined, 2-14-130
- ASW1-ASW2, Contactless - Use Chip Reader, 2-14-152
- ASW1-ASW2 Coding, 2-14-130
- ASW1-ASW2 grouping, 2-14-131
- ASW1-ASW2 Ranges, Local PIN Validation, **2-12-11**
- ATC, 2-5-25, 2-5-26, 2-13-90
- ATR, 2-6-13, 2-6-14
 - ICC, 2-4-9
- Attended, 2-13-72

Audio Indicator, 2-6-6
 Description, 2-4-14, 2-6-5

Auditory environment, 2-6-1

Authorization Advice, 2-5-123
 Definition, **2-13-26**

Authorization Advice Messages
 (0126/0136), 2-13-26

Authorization Code, 2-5-21, 2-5-22,
 2-14-98

Authorization Request, Definition, **2-13-19**

Authorization Response Code, 2-13-86
 Field 55, 2-13-90
 Service Packs, 2-8-4

Authorized Person, 2-7-1

Available Funds, Definition, 2-15-6

Available Offline spending Amount, 2-15-6

B

Backup message, 2-13-81

Base Derivation Key Version, 2-15-47

Batch Number, 2-4-34, 2-5-18, 2-5-88,
 2-14-26, 2-14-57, 2-14-71, 2-14-79,
 2-14-85, 2-14-119
 Definition, 2-15-6
 Requirements, 2-4-34

Battery back-up, 2-6-3

BER-TLV, 2-13-5

Black list, 2-13-81

Business Calls, 2-4-1, **2-4-12**

Business Registration Number, Definition,
 2-15-23

C

CAD Management/Service Quality Data,
2-13-87
 Field 46, 2-13-12, **2-13-87**

CAD output capability, **2-13-67**

CAD security capability, **2-13-67**

Cancel button, 2-5-122, 2-5-123, 2-5-126

Cancellation, 2-4-3, 2-5-84
 Commands, 2-14-117
 Transaction Flow, 2-5-84, 2-5-86

Cancellation Payment, Description,
 2-14-119

Candidate List, 2-4-29, 2-4-32

Capture, 2-5-87

Car Rental, 2-13-81, 2-13-94

Card Action Analysis, 2-5-25

Card balance decreased, 2-13-81

[Card Data], Enciphered, 2-15-7

Card Data, 2-7-1, 2-14-75
 Definition, 2-15-7

Card Data Protection, 2-14-128
 Terminal Settings, 2-15-41

Card Data Source, 2-5-23, 2-5-46, 2-5-63,
 2-5-73, 2-14-55, 2-14-67, 2-14-69,
 2-14-75, 2-14-77, 2-14-83, 2-14-88,
 2-14-117
 Definition, 2-15-7

Card Declined Transactions, Definition,
 2-5-122

Card Handler, Description, 2-4-7

Card inserted correctly?, Merchant Display,
 2-4-25

Card Name, 2-5-25, 2-5-47, **2-13-87**
 Commands, 2-14-37
 Definition, 2-15-7
 for printing, 2-13-86

Card Processing, 2-15-9

Card Product EMV Entry Point Parameters,
 Commands, 2-14-37

Card Product Flow, Commands, 2-14-37

Card Product Functions, Commands,
 2-14-37

Card Product Limits Flags, Commands,
 2-14-37

Card Product Type
 Coding, **2-15-8**
 Commands, 2-14-37
 Definition, 2-15-8

Card Reader error, 2-13-12

Card Readers, 2-3-4

Card Reconciliation Counter ID, 2-13-86

Card Reconciliation Counter Name,
 2-13-86

Card Reference, 2-5-24
 Definition, 2-15-8

Card Related Transactions, 2-4-1

- Card Risk Management, 2-15-42
- Card Selection, 2-3-8, 2-4-7
- Card selection table, 2-3-6
- Card Sequence Number, Definition, 2-15-8
- Card Service Info
 - Coding, **2-15-9**
 - Definition, 2-15-9
 - Get Debit/Credit Properties, 2-14-31, 2-14-32, 2-14-33
- CardData, 2-14-77
- Cardholder Display, 2-4-11, 2-4-13, 2-6-4, 2-14-131, 2-14-132
 - Description, 2-4-10
- Cardholder Initiated Actions, Definition, 2-5-122
- Cardholder Key Pad, Description, 2-4-14
- Cardholder Keyboard, Description, 2-6-6
- Cardholder Verification, 2-5-23
- Cardholder Verification Method, 2-4-5, 2-14-132
- Cash, 2-13-65, 2-15-45
- Cashback, 2-5-20, 2-5-73, 2-15-4
 - Definition, 2-15-9
- CAT, 2-5-91, 2-5-101, 2-6-3
 - Level 1, 2-13-72
 - Level 2, 2-13-70, 2-13-72
 - Level 3, 2-13-70, 2-13-72
- CDA, 2-3-6, 2-3-10
- CDOL1, 2-5-25, 2-15-22
- CDOL2, 2-5-25, 2-15-22
- Central European Time, 2-5-97
- CET, 2-5-97
- CHAP, 2-13-3
- Character height, 2-6-5
- Check Stop List, 2-5-21
 - Description, 2-14-97
- Check Stop List command, 2-5-22
- Check value, 2-5-91, 2-5-106, 2-5-114
 - Handling, **2-5-107**
- Chip Card Reader Design Requirements, 2-6-12
- Clean Up, Complete Payment command, 2-4-6
- Climatic environments, 2-6-1
- CLK pin, 2-6-14
- Clock, Real-time, 2-6-3
- Clock frequency, 2-6-13, 2-6-14
- Clock Synchronization, **2-5-91**, 2-5-124, 2-13-80
 - Definition, 2-13-57
 - Description, 2-5-97
- CNTAID, 2-14-10
- CNTMSC, 2-14-12
- Coding Conventions, 2-13-65
- Coding of Service Packs Supported, **2-15-36**
- Coding of the Length Field, Description, 2-13-6
- Coding of the Value Field, Description, 2-13-7
- Coding of Transaction Options, 2-15-44
- Combined Reader, **2-4-31**, **2-4-32**, **2-4-33**, 2-6-3
- Command - Handler Overview, 2-14-5
- Command Key layout, **2-6-7**
- Command Keys, 2-3-5, 2-6-8
 - Definition, **2-6-9**
 - Description, 2-6-6
- Command Overview, **2-14-1**
- Commands and Responses, Description, 2-14-1
- Commands used during Initialization, 2-14-8
- Communication errors, 2-13-88
 - CAD and the Merchant Application, 2-13-12
 - Public network, 2-13-12
- Communication Handler, Description, 2-4-18
- Communication Protocols, Description, 2-13-2
- Communication Session, Description, 2-5-99
- Communication Statistics, Description, 2-13-12
- Communication Statistics and Error Counters, Exception Handling, 2-5-123
- TI, 2-14-88, 2-14-95
- Token, 2-14-96
 - Complete Payment, 2-14-66, 2-14-73, 2-14-81, 2-14-87, 2-14-121
- Transaction Status, 2-14-65, 2-14-73, 2-14-81, 2-14-87, 2-14-95, 2-14-120

- Complete EMV Payment, 2-5-27
 - Complete Key Entered Payment, 2-5-64
 - Complete Payment, 2-5-47
 - Description, 2-14-65, 2-14-73, 2-14-81, 2-14-87, 2-14-120
 - Complete Payment command, 2-5-115
 - Complete Token Based Payment, 2-5-75
 - Conditions for moving advices to File-5, 2-5-111
 - Configuration, 2-5-11
 - Configuration and installation, 2-5-1
 - Configuration required, 2-5-6
 - Configure PSAM Application, Description, 2-14-15
 - Confirm Amount, 2-5-10
 - Confirm Amount command, 2-5-123, 2-5-126
 - Connection Error Counter, 2-13-17
 - Connection Errors, 2-13-9
 - Connection Request, 2-13-9
 - Connection Request counter, 2-13-16
 - Connection Time counter, 2-13-17
 - Contact force, 2-6-13
 - Contactless
 - Card Data Source, 2-15-7
 - POS Entry Mode, 2-13-72
 - Contactless Terminal Settings, Definition, 2-15-10
 - Contacts, 2-6-4
 - Continuation Indicator, 2-5-11, 2-14-12
 - Continue using magstripe?, Merchant Display, 2-4-25
 - Counters, Example, **2-4-34**
 - Counters and Batch Numbers, Description, 2-4-34, 2-5-109
 - Create Service Record, Description, 2-14-28
 - Cryptogram Information Data, Field 55, 2-13-90
 - CURR, Get Amount 3, 2-14-115, 2-14-116
 - CURRC, Definition, 2-15-10
 - CURRE, Definition, 2-15-10
 - Currency Code, 2-4-10, 2-15-10, 2-15-43
 - Currency Exponent, Definition, 2-15-10
 - Customer Exclusive Data, Field 55, 2-13-90
 - CV-2, 2-14-75, 2-15-7
 - Definition, 2-15-11
 - Field 47, 2-13-89
 - CVC-2, 2-15-11
 - CVM, 2-5-20, 2-5-22
 - CVM Results, 2-5-28
 - Field 55, 2-13-90
 - CVM Status, 2-5-18
 - Coding, **2-15-11**
 - Definition, 2-15-11
 - Service Packs, 2-8-4
 - CVV-2, 2-15-11
- ## D
- Dankort, 2-13-87
 - AID, 2-15-3
 - DAPE, Dankort Accelerated PIN Entry, 2-5-29
 - Data Link Layer, **2-13-2**, 2-13-3
 - Data Management, Description, 2-6-10
 - Data Requested, 2-14-100
 - Coding, **2-15-12**
 - Definition, 2-15-12
 - Data Store, 2-3-6, 2-5-106, 2-5-118, 2-6-9, 2-6-10
 - Data Store Handler, Description, 2-4-18
 - Data Values for Stop List Status, **2-5-15**
 - Date, 2-14-26
 - Date, local transaction, 2-5-88
 - Field 56, 2-13-91
 - DATEPCT, Definition, 2-15-12
 - DCC Amount Extra (CH), Definition, 2-15-12
 - DCC Amount Goods (ME), Definition, 2-15-12
 - DCC Amount Total (ME), Definition, 2-15-12
 - DCC Commission (CH), Definition, 2-15-13
 - DCC Commission (ME), Definition, 2-15-13
 - DCC CURR (ME), Definition, 2-15-13
 - DCC Indicator, Definition, 2-15-13

- DCC Mark Up Exchange Rate, Definition, 2-15-13
 - DCC Reference Date, Definition, 2-15-14
 - DCC Reference Exchange Rate, Definition, 2-15-14
 - DCC Waiter ID, Definition, 2-15-14
 - DDA, 2-3-6, 2-3-10
 - Deactivate PSAM, Description, 2-14-27
 - Debit/Credit Functionality, 2-5-1
 - Debit/Credit Transaction Commands, 2-14-53
 - Default Contactless Application Capabilities, Commands, 2-14-37
 - Default Kernel ID, Definition, 2-15-14
 - Deleting records from File-5, 2-5-113
 - DES, 2-15-20, 2-15-48
 - Design Requirements, 2-6-1
 - Device, 2-6-3
 - Discretionary Data, Get Debit/Credit Properties, 2-14-31
 - Display Line for Host Message, Coding, 2-13-15
 - Display Message Code, Get Amount 3, 2-14-115
 - Display Texts, 2-4-10
 - Displays, 2-3-5
 - Documentation, 2-6-1
 - Download Control
 - Field 27, 2-13-82
 - Position 1, **2-13-82**
 - Download Requirements, 2-6-11
 - Dual Card Reference, Definition, 2-15-15
 - Duplicate Transaction Time-out
 - Definition, 2-15-15
 - Set Debit/Credit Properties, 2-14-42
 - Dynamic Data Authentication, 2-3-6, 2-3-10
- E**
- Eject Button, 2-6-4
 - Electrical Design, Description, 2-6-9
 - Electrical environments, 2-6-1
 - Electrical Interfaces, Description
 - Cards, 2-6-14
 - PSAM, 2-6-13
 - EMV, Card Data Source, 2-15-7
 - EMV Card Transactions, Description, 2-5-23
 - EMV Checksum
 - Definition, 2-15-15
 - Get Debit/Credit Properties, 2-14-32
 - EMV Payment, Description, 2-14-57
 - EMVCo, 2-4-1
 - Enciphered PIN Data
 - Local PIN, 2-14-127
 - Local PIN Validation, 2-12-4
 - End Sentinel, 2-15-22, 2-15-42
 - Entering the Amount, 2-5-17
 - Entry handling, Terminal Settings, 2-15-41
 - Entry Point, 2-15-40
 - Envelope Data
 - Maximum Length (EMV), Get Debit/Credit Properties, 2-14-32, 2-14-34
 - Maximum length (MSC), Get Debit/Credit Properties, 2-14-32
 - Maximum length (non-EMV), Get Debit/Credit Properties, 2-14-34
 - Environmental Requirements, 2-6-1
 - Error Code, Definition, 2-15-16
 - Error Counters, 2-13-12
 - Description, 2-13-12
 - Error Responses, 2-14-7
 - Estimated Amount, 2-15-5
 - Get Amount 3, 2-14-116
 - Europay, AID, 2-15-3
 - Event Handler, 2-5-2, 2-5-122
 - Description, 2-4-19
 - Example of Message Flow, Local PIN Validation, 2-12-11
 - Exception condition - Accumulated Advances, 2-5-110
 - Exception handling, 2-5-106, 2-5-118, 2-5-122
 - Exchange control, 2-13-80
 - Exchange Debit/Credit Static Information, 2-5-8
 - Description, 2-14-18
 - Expiry Date, 2-14-75, 2-15-7

Definition, 2-15-16

Expiry Date (Surface of the Card), Definition, 2-15-17

Extended AID Info, Get Debit/Credit Properties, 2-14-32

Extended AID Info Data, Commands, 2-14-37

Extended Authorization, 2-15-43

Extended Authorization 2, 2-15-43

Extended Issuer Envelope
Set Debit/Credit Properties, 2-14-42
Terminal Settings, 2-15-41

Extended Issuer Envelope Data, 2-13-20, 2-13-21, 2-13-26, 2-13-32, 2-13-38, 2-14-42
Definition, 2-15-17

F

Failed Delivery of Advices, 2-5-111

Fallback, **2-13-70**, 2-14-140
Description, 2-4-24
Final Decision, 2-4-26
POS Entry Mode, 2-13-72

Fallback Handling
Combined Readers, **2-4-31**, **2-4-33**
Separate Readers, **2-4-27**, **2-4-28**

Fallback Handling - ICC Transaction, **2-4-29**

Fallback Handling - Three Strikes, **2-4-30**

FCI, 2-5-24, 2-14-55, 2-15-19
template, 2-5-24

Field 25, 2-13-80

Field 39, 2-5-124

Field 46, 2-5-117, 2-13-103

Field 46 - Messages and related Tags, **2-13-104**

Field 55, 2-13-89

Field 55 for Request and Advice Messages, **2-13-90**

Field 55 for Response Messages, **2-13-91**

Field 72, 2-13-95

File Action Instruction, Definition, 2-13-45

File Action Instruction Acknowledgement, Definition, **2-13-46**

FILEIDADMIN, Definition, 2-15-17

FILEIDPRIORITY,n, Definition, 2-15-17

Final Amount Request, 2-15-5
Get Amount 3, 2-14-115

Final Card Balance, 2-14-64
Definition, 2-15-17

Financial Advice, Definition, **2-13-38**

Financial Advice Messages (0226/0236), 2-13-38

Financial Request, Definition, **2-13-32**

Financial Request Messages (0206/0216), 2-13-32

Firmware Checksum Error, Exception Handling, 2-5-119

Floor limit, 2-13-81

Forced CVM, 2-15-25

Forced offline, 2-5-21, 2-15-25

Forced Online, 2-15-25

Form Factor Indicator, Field 55, 2-13-90

Full reversal, 2-13-80

Function Code, **2-13-79**, **2-13-80**
APACS Header, 2-13-6
Coding, 2-13-14
Field 24, 2-13-79

G

General Requirements, 2-4-1

General transaction flow, **2-10-3**

Generate reconciliation, **2-13-63**, 2-13-80

Generation of a new Host Request, 2-5-119

Get Amount, Subsequent, 2-5-123

Get Amount 2, Service Packs, 2-8-3

Get Amount 3
Description, 2-14-114
Service Pack No. 2, 2-8-5

Get Amount command, 2-5-122, 2-5-126

Get Debit/Credit File Characteristics, Description, 2-14-13

Get Debit/Credit Properties, Description, 2-14-29

Get Debit/Credit Properties Command, Local PIN Validation, 2-12-10

Get Extended Issuer Envelope Contents, Get D/C Properties, 2-14-33

Get Key Check Value 2, 2-14-46

Get Merchant Data, Description, 2-14-100

Get MSC Table, Description, 2-14-11

Get MSC Tracks Information, Get D/C Properties, 2-14-34

Get Next, Description, 2-14-17

Get PIN command, 2-5-123, 2-5-126

Get Processing Condition Table, 2-14-47

Get Random Number, 2-14-44

Get Supported AIDs, Description, 2-14-9

GMT, 2-5-97

GMT Offset
Field 15, 2-13-66
Position 1, **2-13-66**

Goods and Services, 2-13-65, 2-15-45
Cash disbursement, 2-13-65, 2-15-45

Grand Total, Field 46, 2-13-88

Gratuity, 2-15-45

Guard Time, Complete Payment command, 2-4-6

H

Handling of ASWs, Exception Handling, 2-5-116

Hardware Requirements, Description, 2-6-8

Hardware Version Number, 2-5-93,
2-14-18, 2-14-20, 2-14-22
Definition, 2-15-17
Field 46, 2-13-87

HDLC, 2-13-2

Historical Characters, 2-15-31

Host Communication, 2-13-1

Host Declined Transactions (Requests), Exception Handling, 2-5-119

Host Request, 2-14-21, 2-14-23, 2-14-28,
2-14-58, 2-14-62, 2-14-64, 2-14-72,
2-14-80, 2-14-86, 2-14-120
Definition, 2-15-18

Host Response, Definition, 2-15-18

Hotel, 2-13-81, 2-13-94

I

I-Blocks, 2-4-18

ICC, POS Entry Mode, 2-13-72

ICC Power-Off command, 2-5-26

ICC Power-On command, 2-5-2

ICC System Related Data, Field 55,
2-13-89

ID-000 format, 2-6-13

ID-1 format, 2-6-13

Identifier, 2-14-29, 2-14-41
Get Debit/Credit Properties, 2-14-31
Set Debit/Credit Properties, 2-14-42

IDPP, 2-14-16, 2-14-22

IDPPCREATOR, 2-14-16, 2-14-22

IDPSAM, 2-14-9
Definition, 2-15-18
Field 56, 2-13-91

IDPSAMAPP, 2-4-27, 2-4-33, 2-5-1,
2-15-46
Definition, 2-15-18

IDPSAMCREATOR, 2-14-9
Definition, 2-15-18
Field 56, 2-13-91

IDScheme, 2-14-10

IDSN, 2-5-93

IDTHREAD, 2-5-115

IFSC, 2-4-17

IFSD, PSAM, 2-4-17
Value, 2-4-17

IFSF Field 48, 2-13-92

IFSF Field 62, 2-13-92

IFSF Field 63, 2-13-92

Info, 2-4-3

Info Level, 2-5-16, 2-5-89, 2-5-93,
2-14-18, 2-14-20, 2-14-22
Coding, **2-15-19**
Definition, 2-15-18
Field 46, 2-13-87

Initial Amount Request, 2-15-5
Get Amount 3, 2-14-115

Initial Card Balance, 2-14-64
Definition, 2-15-19

Initialization Sequence, Normal flow,
2-5-3

Initiate Cancellation Payment, Description, 2-14-117	2-14-77, 2-14-83, 2-14-88, 2-14-92, 2-14-94
Account Type, 2-14-56, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-89	STAN, 2-14-26, 2-14-56, 2-14-62, 2-14-64, 2-14-68, 2-14-70, 2-14-76, 2-14-78, 2-14-84, 2-14-92, 2-14-118
Action CodePRINT, 2-14-62, 2-14-64, 2-14-92, 2-14-94	Statistics, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-88
AI, 2-14-89	TR, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-88, 2-14-117
Amount, Other, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-89, 2-14-118	Initiate EMV Payment, 2-5-23
Approval Code, 2-14-62, 2-14-64, 2-14-92, 2-14-94, 2-14-98	Initiate EMV Payment 2, Description, 2-14-54, 2-14-88
ARC, 2-14-62, 2-14-64, 2-14-92, 2-14-94	Initiate EMV Payment command, 2-5-24
ATC, 2-14-58, 2-14-86, 2-14-92, 2-14-120	Initiate Key Entered Payment, Description, 2-14-74, 2-14-76
CURRC, 2-14-56, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-89, 2-14-118	Initiate MSC Payment 2, 2-5-46 Description, 2-14-66, 2-14-68
Get Debit/Credit Properties, 2-14-31	Initiate MSC Payment command, 2-5-46
Local PIN, 2-14-124, 2-14-126	Initiate Payment 2 / Account Type, Service Packs, 2-8-8
CURRE, 2-14-56, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-89, 2-14-118	Initiate Token Based Payment 2, Description, 2-14-82
Get Debit/Credit Properties, 2-14-31	Install, Description, 2-14-20
Local PIN, 2-14-124, 2-14-126	Install 2, 2-14-21
CVM Status, 2-14-58, 2-14-72, 2-14-80, 2-14-86, 2-14-120	Install transaction required, 2-5-6
Validate Data, 2-14-62, 2-14-64, 2-14-92, 2-14-94	Installation, 2-5-1, 2-5-10, 2-5-91 , 2-5-117, 2-5-118, 2-13-58, 2-13-80
DATEEFFECTIVE, 2-14-56, 2-14-84, 2-14-92, 2-14-118	Installation guide, 2-6-1
DTHR, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-88, 2-14-117, 2-14-118	Installation Transaction, 2-5-92 Description, 2-5-91
Get Debit/Credit Properties, 2-14-31	Integrated Circuit Card Reader, 2-3-4 Description, 2-6-4
Error Code, 2-14-89	Interface Device (IFD) Serial Number, Field 55, 2-13-90
Kernel ID, 2-14-89	Interface Device Serial Number, 2-5-28
Kernel Specific Data, 2-14-89	Internal PSAM validation, 2-13-80
Kernel Version, 2-14-89	Internet Protocol, 2-13-3
PAN, 2-14-26, 2-14-56, 2-14-68, 2-14-70, 2-14-75, 2-14-76, 2-14-78, 2-14-84, 2-14-92, 2-14-97, 2-14-118	IP, 2-13-3, 2-13-9
Get Amount 3, 2-14-115	Issuer Application Data, Field 55, 2-13-90
Get Debit/Credit Properties, 2-14-31	Issuer Authentication, 2-5-26
PANSEQUENCE, 2-14-56, 2-14-84, 2-14-92, 2-14-118	Issuer Authentication Data, Field 55, 2-13-91
POS Entry Mode, 2-14-55, 2-14-62, 2-14-64, 2-14-67, 2-14-69, 2-14-75,	Issuer DD, Definition, 2-15-19
	Issuer Envelope, Set Debit/Credit Properties, 2-14-42

Issuer Envelope Data
 Definition, 2-15-19
 Field 47, 2-13-89
 Set Debit/Credit Properties, 2-14-42

Issuer Envelope Functionality, Service Pack No. 2, 2-8-7

Issuer Envelope Response Data, Field 44, 2-13-86

Issuer Script, 2-5-26

Issuer Script 1, 2-13-91

Issuer Script 2, Field 55, 2-13-91

Issuer Script Results, Field 55, 2-13-90

Issuer-to-Card Script Processing, 2-5-26

Issuing the Get Amount 2 Command Twice, Service Packs, 2-8-3

Issuing the Get Amount 3 Command Twice, Service Packs, 2-8-5

ITA, 2-4-1

J

JCB, 2-4-34, 2-13-87

K

KCV, 2-15-20
 Card Data Protection, 2-14-128
 Local PIN, 2-15-48

KEK Version, PED, 2-15-47

KEK Version, PSAM, 2-15-47

KEKDATA, Coding, 2-13-14

KEKPIN Version, Field 47, 2-13-89

Kernel ID, Definition, 2-15-19

Kernel Version, Definition, 2-15-20

Key Check Value
 Definition, 2-15-20
 Local PIN, 2-15-48
 Local PIN, 2-14-122, 2-14-128

Key entered
 Card Data Source, 2-15-7
 POS Entry Mode, 2-13-72

Key Entered Card Transactions, Description, 2-5-62

Key Entered Payment, 2-5-63

Description, 2-14-79

Key movement, 2-6-8

Key Type, Card Data Protection, 2-14-128

Keyboard Layout, 2-6-7

KSESDATA, Coding, 2-13-14

KSESPIN, Field 47, 2-13-89

L

LAN, 2-13-2

Landing contacts, 2-6-12

Last PIN incorrect
 Definition, 2-15-48
 Local PIN, 2-14-124, 2-14-126

Leap years, 2-6-3

LENAID, 2-14-118

LENFCI, 2-5-24

Length of APACS 60 Message, Coding, 2-13-14

LENMSCD, Local PIN, 2-14-122, 2-14-124

Limit Info, Definition, 2-15-21

Load Card Data Protection Command, 2-14-128

Load LP Keys Command, 2-14-122
 Local PIN Validation, 2-12-6

Load LP Keys Message Flow, Local PIN, **2-12-5**

Local PIN, 2-12-1
 Application Status Words, 2-12-11
 ASW1-ASW2, 2-14-131
 Limitations, 2-12-10
 Message Codes, 2-12-11
 Message Flow - Magnetic Stripe Cards, **2-12-12**
 PIN Range, 2-12-10

Local PIN Commands, 2-14-122

Local PIN Validation, 2-12-2, 2-14-124
 Description, 2-12-1
 Message flow, 2-12-1

Local PIN Validation Message Flow, **2-12-3**

Local PIN Verification Status, Definition, 2-15-21

Lock, 2-6-4, 2-7-7
 Unattended terminal, 2-7-5

Lodging, 2-13-94

Log, Addendum record, 2-5-89
 Logging Devices, 2-3-6
 LP-KEK
 Definition, 2-15-48
 Local PIN, 2-14-122
 LP-KEK-Data, Local PIN, 2-14-122
 LP-KEK-Version
 Definition, 2-15-48
 Get Debit/Credit Properties, 2-14-32
 Local PIN, 2-14-122, 2-14-123
 LP-Key, Definition, 2-15-48
 LP-Key-Chain
 Definition, 2-15-49
 Local PIN, 2-14-123, 2-14-126
 Local PIN Validation, **2-12-5**
 LP-Key-Chain Structure, Local PIN, **2-12-6**
 LP-Key-Version, Definition, 2-15-49
 LP-PPK, Local PIN, 2-14-122
 LP-PPK-Data, Local PIN, 2-14-122
 LP-PPK-Version
 Get Debit/Credit Properties, 2-14-32
 Local PIN, 2-14-122, 2-14-123, 2-14-126
 LRC, 2-4-8, 2-4-13, 2-15-22, 2-15-42
 Luhn, 2-4-8

M

MAC, **2-5-91**, 2-5-125, 2-13-84, 2-13-85
 MAD-Handler, 2-3-4, 2-6-12
 Description, 2-4-6
 TAPA, 2-3-2
 MAD-Handler ID, 2-5-88, 2-13-89,
 2-14-18, 2-14-20, 2-14-22, 2-14-27
 APACS Header, 2-13-6
 Coding, 2-13-16
 Definition, 2-15-21
 Field 46, 2-13-87
 Maestro, 2-13-87
 Magnetic Stripe, POS Entry Mode, 2-13-70
 Magnetic Stripe Card Reader, 2-3-4
 Description, 2-6-4
 Magnetic Stripe Card Transactions, De-
 scription, 2-5-45
 Magnetic Stripe Contents, Definition,
 2-15-22
 Magstripe Indicator, Definition, 2-15-22
 Mail order, 2-13-72
 Marking, Description, 2-6-2
 Master Card TCC, Field 55, 2-13-90
 MasterCard, 2-4-34, 2-15-11, 2-15-42
 AID, 2-15-3
 Max. PIN digits, Local PIN, 2-14-124,
 2-14-126
 Maximum Deposit, 2-14-64
 Definition, 2-15-22
 Maximum PIN digits, Definition, 2-15-49
 MDOL, Definition, 2-15-22
 MDOL Data, Definition, 2-15-23
 MDOL1, 2-5-17, 2-5-18, 2-14-56, 2-14-57,
 2-14-68, 2-14-70, 2-14-71, 2-14-76,
 2-14-78, 2-14-79, 2-14-84, 2-14-85,
 2-14-119
 MDOL2, 2-5-18, 2-14-58, 2-14-59,
 2-14-72, 2-14-80, 2-14-86
 ME No., **2-5-9**
 MEADDRESS, **2-5-9**, 2-14-19
 Definition, 2-15-23
 MEBRN, **2-5-9**, 2-14-19
 Definition, 2-15-23
 Mechanical Design, Description, 2-6-3
 Mechanical environments, 2-6-1
 MECITY, **2-5-9**, 2-14-19
 Definition, 2-15-23
 MENAME, **2-5-9**, 2-14-19
 Definition, 2-15-23
 MENUMBER, 2-5-30, 2-5-74, 2-14-19,
 2-14-84
 Definition, 2-15-23
 MEPHONE, **2-5-9**, 2-14-19
 Definition, 2-15-24
 Merchant Address, Definition, 2-15-23
 Merchant Application, 2-3-3, 2-5-115
 Description, 2-6-14
 Exception Handling, 2-5-118
 Merchant Application Handler, Description,
 2-4-14
 Merchant Application Log, 2-5-9
 Exchange Debit/Credit Static Informa-
 tion, 2-14-18
 Info Level, 2-15-18
 Install, 2-14-20, 2-14-22

- Merchant Cancel Button, 2-5-125
- Merchant categories, Addendum record, 2-5-87
- Merchant Category Code, **2-5-28**, 2-15-43
- Merchant City Name, Definition, 2-15-23
- Merchant Display, 2-4-25, 2-14-132, 2-15-46
Action Codes, **2-5-125**
- Merchant Identifier, **2-5-28**
- Merchant Initiated Actions, Exception Handling, 2-5-125
- Merchant Initiative, 2-5-87, **2-15-25**
Field 62, 2-13-93
- Merchant Initiative Bypass, 2-9-1, **2-9-3**
- Merchant Name, Definition, 2-15-23
- Merchant Number, Definition, 2-15-23
- Merchant Phone No., Definition, 2-15-24
- Message Code, 2-5-118, **2-5-125**, 2-14-132
Assignments, 2-4-11
Exception Handling, 2-5-123
- Message Number, Field 71, 2-13-93
- Message Reason Code, 2-5-9, **2-13-81**
- Message Size, 2-8-6
- Message Type, **2-13-4**
- Message Type Identifier
APACS Header, 2-13-6
Coding, 2-13-14
Definition, 2-15-26
- Method Number
Definition, 2-15-49
Local PIN, 2-14-122, 2-14-124, 2-14-125, 2-14-126, 2-14-127
- Method Specific Command Data, Local PIN, 2-14-122, 2-14-124
- Method Specific Command Data , Local PIN, 2-14-126
- Method Specific Response Data, Local PIN, 2-14-123, 2-14-125, 2-14-127
- MEZIP, **2-5-9**, 2-14-19
Definition, 2-15-24
- MI, 2-5-21, 2-5-73, 2-5-87, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-88
Definition, 2-15-24
Token, 2-4-4
- Min. PIN digits, Local PIN, 2-14-124, 2-14-126
- Minimum PIN digits, Definition, 2-15-49
- Mode
Coding, **2-15-26**
Definition, 2-15-26
Get Debit/Credit Properties, 2-14-33
- MRC, 2-5-88, 2-14-26
- MSC
Card Data Source, 2-15-7
POS Entry Mode, 2-13-72
- MSC Payment, Description, 2-5-47, 2-14-71
- MSC PIN Retry, Service Pack No. 1, 2-8-3
- MSC Table, 2-5-11
- MSCR, 2-4-8, 2-6-2, 2-6-4
Description, 2-4-7
- MTI, **2-13-4**
Definition, 2-15-26
Field 56, 2-13-91
ISO notation, 2-13-4
- MTI of the Original Message, 2-13-17
APACS Header, 2-13-6
Definition, 2-15-26
- Multi-entry, Terminal Settings, 2-15-41

N

- Nets, 2-15-23
- Nets Debet/Kredit, 2-15-46
- Network Connection Type, 2-13-9
APACS Header, 2-13-6
Coding, 2-13-15
- Network Layer, **2-13-2**, 2-13-3
- Network Management Request, Definition, **2-13-58**
- New application data, 2-5-1, 2-5-10
- New data available, 2-5-7
- New PIN Synchronization, Description, 2-4-19
- No response from Nets, 2-13-12
- Non-volatile, 2-6-11
- NTPIN, 2-14-46
- Number of card reader errors, Field 46, 2-13-88
- Number of Fatal Errors, Field 46, 2-13-88

Number of PIN tries left
 Definition, 2-15-49
 Local PIN, 2-14-124, 2-14-126

Number of System Faults, Field 46,
 2-13-88

Number of time-outs, Field 46, 2-13-88

Number of unsupported cards, Field 46,
 2-13-88

Numeric layout, Keyboard, 2-6-7

O

Odd parity, 2-4-7

Offline Data Authentication, 2-5-23

Offline only terminals, Advice Transfer,
 2-5-102

Online capable terminals, Advice Transfer,
 2-5-102

Online Transactions, Description, 2-5-97

Operation on advices stored in File-5,
 2-5-112

OPT, 2-4-1

Optimizing the Transaction Time, 2-5-29

Original Authorization, Info Level, 2-15-19

Original Data Elements, Field 56, 2-13-91

OTA, 2-4-1

P

Padding, Local PIN, 2-14-127

PAN, 2-5-25, 2-5-47, 2-5-63, 2-5-74,
 2-5-88, 2-15-7
 Definition, 2-15-26
 Get Amount 2, 2-8-3
 Ranges, 2-5-1

PAN Seq. No., Get Amount 3, 2-14-115

PAN Sequence Number, Definition,
 2-15-27

PAN-prefix, 2-3-8
 Get Amount 2, 2-8-3
 Service Packs, 2-8-3

PANFROM, 2-14-12
 Definition, 2-15-27

PANTO, 2-14-12

Definition, 2-15-27

PAP, 2-13-3

Parity, 2-4-13

Partial reversal, 2-13-80

Passenger Transport, 2-13-94

Password, 2-7-6

PCI Data, 2-5-93, 2-14-22
 Definition, 2-15-27
 Field 46, 2-13-88

PCT PANFROM, Definition, 2-15-28

PCT PANTO, Definition, 2-15-28

PDOL, 2-5-27, 2-8-3

PED, 2-3-2, 2-3-7

PED BDK Version, 2-14-22

PED Data, 2-5-93, 2-14-22

PED KEK
 Derivation Data, 2-14-22

PED Software, 2-6-10

Physical Layer, **2-13-2**, 2-13-2

Pick up, 2-14-149

Pick-up, 2-14-98, 2-15-38

Pictograms, 2-6-2
 Examples, 2-6-2

PIN, 2-5-122
 Capture, 2-13-69
 Capture capability, **2-13-67**
 Data, Definition, 2-15-29
 Privacy, 2-6-8
 Retry, 2-5-119, 2-8-3
 Tries, Local PIN, 2-12-10

PIN Block Format
 Coding, **2-15-29**
 Definition, 2-15-28
 Field 47, 2-13-89
 Get Debit/Credit Properties, 2-14-33
 Terminal Settings, 2-15-41

PIN Entry, 2-4-5, 2-5-24, 2-5-46
 Device, 2-3-5, 2-7-1
 Numeric Keys, 2-7-3

PIN Pad, 2-13-71
 Software, 2-6-11
 Description, 2-6-6
 Design, 2-6-3
 Field 46, 2-13-87

PIN Pad Data, Storage, 2-6-11

PIN Pad layout, 2-6-7

- PIN Pad Software, 2-6-12
- PIN Pad/PSAM Key Synchronization, Terminal Settings, 2-15-41
- Exception Handling, 2-5-115, 2-5-117, 2-5-119
 - Description, 2-5-115
- PIN Retry Flow, Exception Handling, **2-5-121**
- PIX, 2-15-3
- Plaintext PIN Block, **2-12-4**
 - Local PIN, 2-14-127
- Plaintext PIN Data, Local PIN Validation, 2-12-4
- POS Capability, **2-13-73**
- POS Capability Code, 2-5-93, 2-14-18, 2-14-20, 2-14-22
 - Definition, 2-15-29
 - Field 21, 2-13-66
 - Position 1, **2-13-66**
 - Position 2, **2-13-67**
 - Position 3, **2-13-67**
 - Position 4, **2-13-67**
 - Position 5, **2-13-67**
 - Position 6, **2-13-68**
- POS Capability Codes, **2-13-75, 2-13-79**
- POS Entry Mode, 2-4-25, 2-5-20, **2-5-28, 2-13-73, 2-13-75, 2-13-79**
 - Definition, 2-15-29
 - Field 22, 2-13-70
 - Initiate Payment command, **2-13-72**
 - Position 1, **2-13-70**
 - Position 2, **2-13-70**
 - Position 3, **2-13-70**
 - Position 4, **2-13-71**
 - Position 5, **2-13-71**
 - Position 6, **2-13-71**
 - Service Packs, 2-8-4
- POS terminal, 2-6-3
- Post Purchase, 2-15-43
- Post Refund, 2-15-43
- Postal Code, 2-15-24
- Power failure, 2-6-4, 2-6-9
- Power On, Description, 2-5-2
- Power supply, 2-6-13, 2-6-14
- Power-on, Type of Application, 2-15-46
- PPP, 2-13-3
- PPS, 2-6-13, 2-6-14
 - ICC, 2-4-9
- Presentation layer, **2-13-2**
- Previous Transaction Status, Get Debit/Credit Properties, 2-14-31
- Primary Account Number, 2-15-26
- Primary and Secondary Access Points, 2-13-1
- Printer, 2-4-14
- Privacy Shield, 2-7-1
 - Figures, 2-7-8
 - Height and position of the PED, **2-7-12**
 - Height of the Shielding, **2-7-10**
 - Mounting of the PED, **2-7-11**
 - PIN Entry Device, **2-7-8**
 - Reference Directions, **2-7-9**
 - Size and Orientation, 2-7-2
- Privacy Shield around the PIN Entry Device, **2-7-8**
- Private Label Card, 2-11-2
- Private Label Card Scheme, 2-15-9
- Problem Reporting, Description, 2-10-1
- Processing Code, Field 3, 2-13-65
- Processing Option Data Object List, 2-5-27
- Processing Restrictions, 2-5-23
- Properties / Data Elements to be Requested, **2-14-31**
- Properties / Data Elements to be Set, Set Debit/Credit Properties, **2-14-42**
- Proprietary Application Identifier Extension, Definition, 2-15-3
- Proprietary Data
 - APACS Header, 2-13-6
 - Coding, 2-13-16
- Protected access to Card Reader and PIN Entry Device, 2-7-4
- Protocol Layers, **2-13-2**
- Protocols, Description, 2-13-1
- Proximity Payment, POS Entry Mode, 2-13-70
- PSAM Behavior for Variants of different Get Amount Commands, **2-8-7**
- PSAM busy, 2-5-119
- PSAM Card Reader(s), Description, 2-6-12
- PSAM clean-up, 2-5-115
- PSAM Code Checksum, Definition, 2-15-29
- PSAM Config Checksum, Definition, 2-15-30

PSAM D/C Life Cycle State
 Definition, 2-15-30
 Get Debit/Credit Properties, 2-14-31

PSAM Date, Field 46, 2-13-88

PSAM deactivation, **2-5-91**, **2-5-97**,
2-13-80
 Definition, 2-13-62
 Description, 2-5-96

PSAM Declined Offline Transactions, Definition, 2-5-122

PSAM Declined Online Transactions, Definition, 2-5-122

PSAM Handler, Description, 2-4-16

PSAM ID
 APACS Header, 2-13-6
 Coding, 2-13-14
 Field 60, 2-13-92

PSAM Identifier, Get Debit/Credit Properties, 2-14-31

PSAM Life Cycle State, Field 46, 2-13-88

PSAM Parameters, 2-15-30
 Field 46, 2-13-88

PSAM Related Errors, Exception Handling, 2-5-118

PSAM Scripts, 2-5-98

PSAM Security Configuration, Get Debit/Credit Properties, 2-14-35

PSAM Shutdown
 Command, 2-5-118
 Description, 2-5-14

PSAM Software, 2-6-12

PSAM State Information, 2-5-9
 Exchange Debit/Credit Static Information, 2-14-18
 Install, 2-14-20, 2-14-22

PSAM Subversion
 Definition, 2-15-30, 2-15-31
 Get Debit/Credit Properties, 2-14-31

PSAM Update, **2-5-91**, **2-5-96**, **2-13-80**
 Definition, 2-13-61
 Description, 2-5-93, 2-14-52
 Exception Handling, 2-5-119
 Extracting the commands, **2-5-94**
 Field 63, 2-13-93
 Messages, **2-13-45**

PSAM Update Flag, 2-5-98, 2-13-6,
 2-13-15

PSAM Version
 Definition, 2-15-31
 Field 46, 2-13-88
 Get Debit/Credit Properties, 2-14-31

PSAM/PIN Pad Synch. Sequence, 2-5-13

PSAM/PIN Pad synchronization, 2-5-1,
 2-5-12

PSAMs, TAPA, 2-3-2

PTS Request Data, Field 46, 2-13-88

PTS Response Data, Field 46, 2-13-88

Q

Quasi-cash and scrip, 2-13-65, 2-15-45

R

Random Number, 2-5-106, 2-5-111,
 2-5-112
 Field 61, 2-13-93

Random Pad Pattern, Local PIN, 2-14-127

Receipt Printer, 2-3-5
 Description, 2-6-9

RECON_CounterID, Definition, 2-15-33

RECON_CounterNAME, Definition, 2-15-33

RECON_PANFROM, Definition, 2-15-34

RECON_PANTO, Definition, 2-15-34

Reconciliation, 2-13-63

Reconciliation counter id, **2-13-86**
 Description, 2-4-34

Reconciliation counter name, 2-13-86
 Description, 2-4-34

Reconciliation Data, 2-13-93

Reconciliation date, Description, 2-4-34

Reconciliation id, **2-13-86**

Reconciliation Indicator, Description,
 2-4-34

Reconciliation report, **2-13-63**, 2-13-80

Reference STAN, 2-13-17
 APACS Header, 2-13-6
 Definition, 2-15-34
 Get Debit/Credit Properties, 2-14-31

Registered Application Identifier, 2-15-3

Rejection tone, 2-6-6

Release of the ICC, 2-5-31

Repeat Last ICC Response, 2-4-9
Description, 2-14-104
FCI, 2-5-24

Repeat Messages, 2-5-98

Reset , CAD, 2-4-23

Response Code, 2-4-9, 2-5-123, 2-5-126,
2-8-4

Response time for previous online transaction, Field 46, 2-13-87

Restart, 2-5-1
Description, 2-5-6

Restart required, 2-5-7

Retrieval Reference Number, 2-4-34

Retrieve
Advice Information, Get Debit/Credit Properties, 2-14-35

Retrieve Acquirer Information, Get D/C Properties, 2-14-33

Retrieve Available Funds Amount, Get D/C Properties, 2-14-33

Retrieve Contactless Amounts, Get Debit/Credit Properties, 2-14-33

Retrieve Hash Value, 2-14-35

Retrieve Local PIN Information, Get Debit/Credit Properties, 2-14-32

Retrieve Reference STAN, Get Debit/Credit Properties, 2-14-32

Retrieve Security Information, Get D/C Properties, 2-14-33

Retrieve TVR/TSI/IAC, Get Debit/Credit Properties, 2-14-32

Returns/Refunds, 2-13-65, 2-15-45

Reversal, 2-5-117
Advice, 2-5-122
Definition, **2-13-47, 2-13-48**

Reversal (Authorization), 2-4-4

Reversal Advice Messages (0426/0436), 2-13-47

RID, 2-15-3
PSAM, 2-13-91, 2-14-9

RIDPSAM, Definition, 2-15-2, 2-15-6,
2-15-7, 2-15-21, 2-15-27, 2-15-34,
2-15-46

Router

Description, 2-4-6
TAPA, 2-3-1

S

Salt, 2-15-34, 2-15-35

Scheme Id, 2-15-35

Scheme Id Bitmap, 2-15-35

SDA, 2-3-6

Secure Device, 2-14-154

Security Mechanism, 2-5-106

Security Zones, **2-3-9**, 2-3-9

Seed, 2-14-69, 2-14-77
Definition, 2-15-35
Get Debit/Credit Properties, 2-14-33

Segment Number, 2-15-46

Selectable Kernel Configurations
Definition, 2-15-35
Set Debit/Credit Properties, 2-14-42

Selection of Service Packs supported,
2-8-1

Separate Reader, 2-4-27, 2-4-28

Service Code, 2-4-26, 2-15-9
Definition, 2-15-36
Get Debit/Credit Properties, 2-14-31,
2-14-32, 2-14-33

Service life, 2-6-4

Service Pack Check, **2-5-8**

Service Pack No. 1, 2-8-3

Service Pack No. 2, 2-8-5

Service Packs, 2-8-1
Restart, 2-5-7

Service Packs Overview, **2-8-2**, 2-8-2

Service Packs Supported
Definition, 2-15-36
Get Debit/Credit Properties, 2-14-31

Service Record, 2-5-95, 2-5-119, 2-13-56,
2-13-80

Servicing the Terminal, 2-6-3

Session Layer, **2-13-2**, 2-13-3

Set Debit/Credit Properties, 2-5-8
Service Pack No. 2, 2-8-7

SettingsCL, Definition, 2-15-36

SHA-1, 2-5-106

- Shielding
 - Design Recommendations, 2-7-3
 - Size and orientation, 2-7-2
 - Shoulder Surfing, 2-7-1
 - Shut-down, 2-5-118
 - Shutter, 2-6-4
 - Signature, 2-4-5
 - Signature accepted, 2-5-19
 - Signature Status, 2-14-99
 - Signature Verification
 - Coding, **2-15-37**
 - Definition, 2-15-37
 - Signature Verification Function, 2-4-5
 - SignTOPUP, 2-14-64
 - Single-entry, Terminal Settings, 2-15-41
 - Sliding contacts, 2-6-12
 - Software Design, Description, 2-6-10
 - Software download, 2-6-12
 - Software Version Number, 2-5-93, 2-14-18, 2-14-20, 2-14-22
 - Definition, 2-15-37
 - Field 46, 2-13-87
 - STAN, 2-5-88, 2-5-120, 2-13-87
 - Definition, 2-15-37
 - STANREF, 2-14-118
 - Start Sentinel, 2-15-22, 2-15-42
 - Start-up, 2-5-117, 2-5-118
 - Start-up PSAM, 2-5-6
 - Description, 2-14-8
 - State Information, 2-14-102
 - Static Data Authentication, 2-3-6
 - Statistic Vector, 2-13-16, **2-13-18**
 - Statistics, 2-13-6, 2-13-8
 - Candidates tags, 2-13-88
 - Coding, 2-13-16
 - Definition, 2-15-38
 - Description, 2-13-12
 - Initiate EMV Payment, 2-5-17
 - STIP, 2-4-1
 - Stop List, 2-5-14, 2-5-21, 2-5-122
 - Electronic data file, 2-5-21
 - Manual look up, 2-5-21
 - Stop List check, 2-5-25
 - Stop List Status, 2-5-21, 2-14-98
 - Coding, **2-15-38**
 - Definition, 2-15-38
 - Storage of Data, Description, 2-6-11
 - Storage of Data Elements, **2-5-28**
 - Storage of Software, 2-6-11
 - Structure of the Tag Field, 2-13-5
 - Submit Card Reference, Description, 2-14-105
 - Submit Initial Key 2, 2-14-24
 - SUBVERSIONPCT, Definition, 2-15-38
 - Supplementary Authorization, 2-14-86
 - Synchronization, 2-5-12
 - Synchronization Algorithm and Key Length, 2-15-4
 - Synchronize PSAM/PIN Pad, Description, 2-14-16
 - System Overview, 2-3-1
 - System Trace Audit Number, 2-15-37
 - Systems Trace Audit Number, 2-5-88, 2-5-120, 2-13-14
 - APACS Header, 2-13-6
 - Field 56, 2-13-91
- ## T
- Tag
 - 4F, 2-13-90, 2-15-3
 - 50, 2-15-5
 - 57, 2-13-19, 2-13-32, 2-13-38, 2-13-40, 2-13-47, 2-13-49
 - 5F24, 2-13-19, 2-13-90, 2-15-16
 - 5F2A, 2-13-90
 - 6F, 2-5-24
 - 70, 2-14-143
 - 71, 2-13-91
 - 72, 2-13-91
 - 82, 2-13-90
 - 84, 2-15-3
 - 8A, 2-13-90
 - 91, 2-13-91
 - 95, 2-13-90
 - 9A, 2-13-88, 2-13-90
 - 9B, 2-13-88, 2-13-90
 - 9C, 2-13-88, 2-13-90
 - 9D, 2-13-88
 - 9F02, 2-13-90
 - 9F03, 2-13-90
 - 9F09, 2-13-90

9F10, 2-13-90
 9F1A, 2-13-90
 9F1B, 2-14-37
 9F1C, 2-15-40
 9F1E, 2-13-90
 9F26, 2-13-90
 9F27, 2-13-90
 9F33, 2-13-90
 9F34, 2-13-90
 9F35, 2-13-90
 9F36, 2-13-90
 9F37, 2-13-90
 9F41, 2-13-90
 9F4B, 2-14-137
 9F53, 2-13-90, 2-15-42
 9F6E, 2-13-90
 9F7C, 2-13-90
 A3, 2-13-86
 A4, 2-13-86
 A5, 2-13-86
 Application Version Number, 2-13-90
 BE, 2-13-89
 BF, 2-13-89
 BF0C, 2-15-19
 BG, 2-13-86
 BH, 2-13-86
 C0, 2-13-6, 2-13-14
 C1, 2-13-6, 2-13-14
 C2, 2-13-6, 2-13-14
 C3, 2-13-6, 2-13-14
 C4, 2-13-6, 2-13-14
 C5, 2-13-6, 2-13-14
 C6, 2-13-6, 2-13-14
 C7, 2-13-6, 2-13-14
 C8, 2-13-6, 2-13-15
 C9, 2-13-6, 2-13-15
 CA, 2-13-6, 2-13-15
 CB, 2-13-6, 2-13-8, 2-13-9, 2-13-15
 CC, 2-13-6, 2-13-16
 CD, 2-13-6, 2-13-16
 CE, 2-13-6, 2-13-16
 CF, 2-13-6, 2-13-8, 2-13-16, 2-13-18
 D0, 2-13-90
 D1, 2-13-6, 2-13-17, 2-15-34
 D2, 2-13-6, 2-13-17
 DF70, 2-14-37
 DF71, 2-14-37
 DF72, 2-14-37, 2-15-8
 DF73, 2-14-37
 DF76, 2-14-37
 E0, 2-13-6
 E2, 2-13-6
 E4, 2-14-37
 I1, 2-13-65
 IM, 2-13-65
 T1, 2-13-86
 T2, 2-13-87
 T3, 2-13-87
 T4, 2-13-87
 T5, 2-13-87
 T6, 2-13-87
 T7, 2-13-87
 T9, 2-13-87
 TA, 2-13-87
 TB, 2-13-87
 TC, 2-13-87
 TD, 2-13-87
 TE, 2-13-13, 2-13-88
 TF, 2-13-13, 2-13-88
 TG, 2-13-88
 TH, 2-13-13, 2-13-88
 TI, 2-13-88
 TJ, 2-13-88
 TK, 2-13-88
 TL, 2-13-89
 TM, 2-13-89
 TN, 2-13-89
 TO, 2-13-93
 TP, 2-13-88
 TQ, 2-13-88
 TR, 2-13-88
 TS, 2-13-88
 TW, 2-13-93
 TX, 2-8-8, 2-13-89
 TY, 2-8-8, 2-13-86
 V5, 2-13-89
 TAGAdditionalInfo, Definition, 2-15-38
 Tags, Messages and related Tags,
2-13-103
 Tamper Response, 2-6-8
 TAPA, 2-3-1, 2-4-1, 2-5-1, 2-5-14, 2-5-23,
 2-14-7
 TAPA Architecture, Local PIN, **2-12-2**
 TAPA Model, 2-3-2
 TAPA PSAM Application Identifier, Defini-
 tion, 2-15-18
 Tapping Device, 2-7-1
 Countermeasure, 2-7-6
 TC, 2-5-25, 2-13-90
 TCP, 2-13-3, 2-13-9
 Tearing, 2-13-81
 Telephone order, 2-13-70, 2-13-72
 Terminal, Physical Implementation, **2-3-3**
 Terminal Action Analysis, 2-5-25
 Terminal Approval No., 2-5-88, 2-5-93,
 2-14-18, 2-14-20, 2-14-22, 2-14-26,
 2-14-27

- Coding, **2-15-39**
- Definition, 2-15-38
- Field 46, 2-13-87
- Service Packs, 2-8-1
- Terminal Architecture for PSAM Applications (TAPA), **2-3-1**
- Terminal Capabilities, **2-5-28**, 2-5-93, 2-14-18, 2-14-20, 2-14-22
 - Field 46, 2-13-87
 - Field 55, 2-13-90
- Terminal Checksum
 - Definition, 2-15-39
 - Get Debit/Credit Properties, 2-14-32
- Terminal Contactless Floor Limit
 - Commands, 2-14-37
 - Definition, 2-15-39
- Terminal Contactless Transaction Limit
 - Commands, 2-14-37
 - Definition, 2-15-39
- Terminal Country Code, Field 55, 2-13-90
- Terminal CVM Required Limit
 - Commands, 2-14-37
 - Definition, 2-15-39
- Terminal Data, Storage, 2-6-11
- Terminal Decision Flags
 - Coding, **2-15-40**
 - Definition, 2-15-40
- Terminal Floor Limit, 2-5-28
- Terminal Identification, 2-5-17, 2-5-28, 2-5-88, 2-5-93, 2-14-26, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83, 2-14-88
 - APACS Header, 2-13-6
 - Coding, 2-13-16
 - Definition, 2-15-40
- Terminal Manufacturer ID, 2-13-89, 2-15-21
 - Definition, 2-15-40
- Terminal Merchant Table, **2-5-9**
- Terminal Model, 2-3-1
- Terminal Operator, 2-6-11
- Terminal Operator Communication Access Points, 2-5-100
- Terminal Related Errors, Exception Handling, 2-5-117
- Terminal Serial Number, 2-13-89, 2-15-21
 - Definition, 2-15-41
- Terminal Settings, 2-5-8
 - Coding, **2-15-41**
 - Definition, 2-15-41
 - Set Debit/Credit Properties, 2-14-42
- Terminal Software, 2-6-11
- Terminal Software Modules, 2-6-12
- Terminal Transaction Qualifiers, Commands, 2-14-37
- Terminal Type, 2-5-93, 2-14-18, 2-14-20, 2-14-22
 - Field 46, 2-13-87
 - Field 55, 2-13-90
- Terminal Verification Result (TVR), Field 55, 2-13-90
- Terminals supporting prepaid cards, Advice Transfer, 2-5-103
- Terminals using Dial-up, Advice Transfer, 2-5-103
- The fifth File (File-5), 2-5-111
- Third Party Data/Device Type Indicator, Field 55, 2-13-90
- TI, Definition, 2-15-43
- Time, 2-14-26
 - Definition, 2-15-50
- Time-out, 2-5-123, 2-8-4, 2-13-81
 - Exception Handling, 2-5-126
- Time, local transaction, 2-5-88
 - Field 56, 2-13-91
- Timer Flag, Definition, 2-15-50
- TLV, 2-5-17, 2-5-27, 2-13-89
 - Coding, 2-13-5
- TO, 2-15-44
- Token, 2-4-3
 - Card Data Source, 2-15-7
 - Definition, 2-15-41
 - Format of the Token, 2-4-3, **2-4-4**
 - Maximum length, 2-4-3
 - POS Entry Mode, **2-13-72**
- Token Based Payment, Description, 2-14-85
- Token based transaction flag, 2-13-89
- Token based Transactions, 2-5-72
- Top up, 2-15-43
- Top Up Amount, 2-14-64
- Total Issuer Envelope buffer sizes, Get Debit/Credit Properties, 2-14-34

- TR, 2-5-16, 2-15-43
- Track 1, 2-14-34
- track 2, 2-5-46
- track 3, 2-4-7, 2-5-46
- [Track Data], Enciphered, 2-15-42
- Track Data, 2-14-67
Get Debit/Credit Properties, 2-14-33
- Track1, 2-4-7
- Track1 Data, 2-15-42
- Track2, 2-4-7, 2-4-8, 2-5-62, 2-14-67
Data, 2-15-22
Definition, 2-15-42
Get D/C Properties, 2-14-34
- Track2 Data, Get Debit/Credit Properties, 2-14-31
- Track3, 2-4-7, 2-14-67
Data, Definition, 2-15-42
Get D/C Properties, 2-14-34
- Track3 Data, Get Debit/Credit Properties, 2-14-31
- TrackData, 2-14-69
- Transaction Category Code, Definition, 2-15-42
- Transaction Counter
Definition, 2-15-50
Get Debit/Credit Properties, 2-14-32
Local PIN, 2-14-127
- Transaction Counter Validation, Local PIN Validation, 2-12-7
- Transaction Currency Code, Field 55, 2-13-90
- Transaction Date, Field 55, 2-13-90
- Transaction flow, 2-4-1
- Transaction Gratuity Amount, Definition, 2-15-43
- Transaction Identifier, Definition, 2-15-43
- Transaction Option, 2-15-44
- Transaction Processing, 2-5-16
- Transaction Request, 2-13-17
Coding, **2-15-43**
Definition, 2-15-43
- Transaction Sequence Counter, Field 55, 2-13-90
- Transaction Sequence Number, 2-5-28
- Transaction State Information, 2-5-19, 2-15-19
Coding, **2-15-44**
Command, 2-5-23
Definition, 2-15-44
Description, 2-14-102
- Transaction Status, 2-4-5, 2-5-19, 2-5-89, 2-5-115
Coding, **2-15-45**
Definition, 2-15-45
- Transaction Status Information, Field 55, 2-13-90
- Transaction Time, 2-5-28
- Transaction Total Amount, Definition, 2-15-45
- Transaction Type, 2-5-17, **2-5-28**
Definition, 2-15-45
Field 55, 2-13-90
- Transfer of Advices from support system, 2-5-114
- Transferring Advices, Description, 2-5-101
- Transmission Flows, 2-13-3
- Transmission Formats, Description, 2-13-4
- Transport Layer, **2-13-2**, 2-13-3
- Truncated PAN
Definition, 2-15-45
Get D/C Properties, 2-14-34
- TS PED KEK, 2-15-46
- TSI, **2-5-28**, 2-13-90
- TT, 2-5-17, 2-14-55, 2-14-67, 2-14-69, 2-14-75, 2-14-77, 2-14-83
Definition, 2-15-45
- TVR, **2-5-28**, 2-13-90
- Type of Application, Definition, 2-15-46
- ## U
- Unique serial number, 2-6-2
- Unpredictable Number, 2-5-28
Field 55, 2-13-90
- Unsupported cards, 2-13-12
- Update Data, 2-14-52
Definition, 2-15-46
- Update Number, 2-14-52
Definition, 2-15-46
- Update Results, Field 46, 2-13-87

UPT, 2-5-98
User Guidance, 2-6-2
User Interface, 2-5-126
User Interface Handler, Description,
2-4-10

V

V.110, 2-13-2
V.120, 2-13-2
Valid values for Field 21 (POS Capability
Code), 2-13-69
Acquirer Name, 2-14-94
Card Name, 2-14-56, 2-14-68, 2-14-70,
2-14-76, 2-14-78, 2-14-84, 2-14-118
Get Debit/Credit Properties, 2-14-31,
2-14-33
Host Response, 2-14-23, 2-14-59, 2-14-93
ME-No, 2-14-94
Segment Number, 2-14-59, 2-14-93
Application Chaining, 2-14-61
Validate Data, 2-5-26, 2-5-47, 2-5-64
Validate Data 2, 2-14-59
Service Pack, 2-8-4
Validate Install Data, Description, 2-14-23
Validate Install Data command, 2-5-93
Vehicle Rental, 2-13-94
Verify Signature, Description, 2-14-99
Verify Signature command, 2-5-19
VERSIONPCT, Definition, 2-15-46
Viewing angle, **2-6-5**
Visa, 2-15-11
AID, 2-15-3
Visual Indicators, Description, 2-6-4
VK, 2-14-128
Card Data Protection, 2-14-128
VK PED KEK, 2-15-47
VK PSAM KEK, 2-15-47
VKBKD, 2-15-47
VKKEK, Card Data Protection, 2-14-128
Voice Authorization, 2-5-22, 2-14-98,
2-15-38
VPN, 2-13-2

W

Waiting Time Extension, 2-4-17
WTX, PSAM, 2-4-17

X

X.75, 2-13-2

Z

ZIP code, 2-15-24

This page is intentionally left blank