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 authorised 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 1-10-7.

1-9.5 Support of Card Technologies

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

- ICC (Contact)
- Magnetic Stripe (Track 2)
- Key-Entered and
- Contactless (ICC/MSD/Mobile device)

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

References

Card Data Source, definition: Section 2-15.2.23 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 2-4-25.

Card inserted correctly: Section 2-4.17.2 on page 2-4-25.

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 may support Service Pack 2 or Service Pack 3. The functionality of Service Pack 3 should be used for new terminals.

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

Application Selection is, for contactless transactions performed by the kernels loaded in terminal. The processing based on information loaded from the PSAM into the terminal.

The PSAM will, as of Service Pack 3, perform application selection for all other contact transactions. The selection is based on information from the administration system. The selection includes possibility for cardholder selection as required in the IFR from the EU.

When an ICC card is inserted in the terminal, the PSAM builds a 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 may decide which application to be used. This selection shall be performed as a dialog between the cardholder and the terminal. The Issuer and the Merchant may have preferred applications but the Cardholder performs the final decision. 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 in the same way as during a Purchase(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 1-14-11.

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.

NOTE: This is normally only allowed during a start up phase of implementing chip and PIN.

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 2-15.2.94 on page 2-15-25.

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 2-15.2.94 on page 2-15-25.

1-9.11 Voice Authorisation Calls

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

A Voice Authorisation 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 alpha-numeric characters.

The request for Voice Authorisation 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 Authorisation Call may either be:

- No Voice Authorisation Call Performed,
- No Voice Authorisation Call Performed, but the card number is found in the Stop List.
- Voice Authorisation Call performed, but the authorisation request has been declined,
- Voice Authorisation Call performed, and the authorisation request has been approved.

If the manual authorisation 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 Authorisation Call Performed) may be given.

In order to obtain a Voice Authorisation, the PAN must be known. The expiry date and the CVV2 may also be needed. During the transaction, the PSAM/Terminal will, for non-PCI cards, 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 Authorisation Call is performed before the transaction is initiated, the PAN embossed/printed on the front of the card or a PAN printed on the reverse side of the card will be used.

References

Voice Authorisation: Section 2-5.5.5 page 2-5-26, EMV Payment and section 2-5.7.4 page 2-5-50, 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 only select to request a look up on the Stop List in the following situation:

- If the transaction is processed forced 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 2-14.6.27 on page 2-14-131.

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, i.e. entry of PIN may start before the the amount is known.

Two different variants of "Accelerated PIN Entry - APE" 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 2-5-32, 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 2-5-34, 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 2-5-31.

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.

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

If the PIN was offline validated (early in the transaction sequence) the terminal must print a receipt (covering the PIN entry attempt).

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 non contactless 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 2-14.193 on page 2-14-184.

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 2-5.15.1 page 2-5-116, General Rules and section 2-14.10 page 2-14-183, 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 1-10-31, 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 shall 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 amount shall use the same Currency Code as used for the total transaction amount.

It is not allowed to combine cashback with:

- DCC
- Key Entered transactions

When Cashback is indicated in Amount Other, the Transaction Type (TT) shall for non-contactless transaction be set accordingly to '09' (Goods and services with cash disbursement). The terminal shall, for contactless transactions set Transaction Type according to the rules of the individual card scheme.

References

Cashback, definition: Section 2-15.2.11 page 2-15-4, Amount, Other.

1-9.19 Addition of Surcharges and Fees

The merchant (or if automatically, the Cash Register) may add surcharge 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 surchanges and other fees.

References

NOTE: The Payment Service Directive 2 will limit the possibility of the use of surcharge.

Surcharges and Fees: Section 1-10.18 page 1-10-125, 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.

NOTE: It is, due to the EU PSD2 directive no longer allowed to charge surcharge or fees to the cardholder for intra EEA transactions on private cards.

References

Surcharges and Fees: Section 1-10.18 page 1-10-125, 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. 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 2-5.13.5 page 2-5-101 and Dual access points: Section 2-13.3 page 2-13-2, Communication Protocols.

See also chapter 2-5.13, Online Transaction and chapter 2-5.14, Transferring Advices.

1-9.22 Balancing and the Transfer of Advices

The transfer of advices is automatically controlled by the terminal, see chapter 2-5.14 page 2-5-102, 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 2-5.14 page 2-5-102.

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 1-9-26, Total Reports and section 1-9.25 page 1-9-17, 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.

NOTE: The Merchant Application Log has been disabled due to the PCI PA-DSS requirement "do not sote sensitive data, even if encrypted".

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

The data elements can be retrieved in the response from the *Validate Data 3* command, part of Service Pack 3 (SP3)

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-periods. 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 2-4-35, 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,
- Visa,
- 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	001 (DANKORT)	180120	000
		180121	000
	200 (MASTERCARD)	180121	001
			002
			003
			004
		180122	001
			002
	203 (DINERS)	180122	001
			002
2	200 (MASTERCARD)	180121	001
			002
			003
			004
		180122	001
	203 (DINERS)	180122	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 in-

formation 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 card-

holders 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 2-14.6.30 page 2-14-136.

1-9.28 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.

1-9.28.1 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 unauthorised 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.

1-9.28.2 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.

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.

This page is intentionally left blank