

ERRATA to:

Terminal Architecture for PSAM Applications
(TAPA)

Application Architecture Specification

Version 2.1

February 2001

*version 1.1
2004-03-12*

Purpose of this document and notation used

This document is intended as errata to the existing TAPA Application Architecture specification, version 2.1.

The present document summarizes all clarification, modification or correction discovered since the TAPA specification was released.

All comments are stated individually.

If extensive information has been added, this information is stated on the last pages of the present document. New information stated on the last pages, is stated with a reference to the item, to which it concerns.

Whenever a modification to the text or wording used in the TAPA specification, is stated in the present document, the following notation is used:

~~Crossed text~~: Indicates that existing text in the TAPA specification shall be deleted or substituted.

Italic text: Indicates that a new text string shall be added (or shall substitute an existing text) in the TAPA specification.

Item	Date Added	Specification References	Description
1	2001-11-05	Table 60 (page 68)	<p>Correction</p> <p>Three of the Response Codes shown in table is not relevant in the response to "Get Key Check Value" command.</p> <p>The following three values shall be removed from Table 60:</p> <p>'FF91' Certificate format error 'FF92' Certificate expired 'FF93' Certificate ID mismatch</p>
2	2001-11-05	Table 68 (page 73)	<p>Correction</p> <p>The three values for Response Code deleted in table 60 (see item number 1) shall be added to table 68 instead:</p> <p>... ... 'FF90' RSA key mismatch, VKP not recognized 'FF91' <i>Certificate format error</i> 'FF92' <i>Certificate expired</i> 'FF93' <i>Certificate ID mismatch</i> 'FFF3' Handler Error </p>
3	2001-11-05	Table 109 (page 113)	<p>Substantive Addition</p> <p>The range of SW1 SW2 needs to be augmented in order to handle errors while chaining.</p> <p>The following two rows shall be added to tabel 109:</p> <p><i>SW1 SW2 '6F01' Syntax error in command. Resend command.</i></p> <p><i>SW1 SW2 '6F02' Syntax error in command</i></p>

Item	Date Added	Specification References	Description
4	2001-11-05	Section 7.2.1 (page 67)	<p>Clarification</p> <p>The existing requirement 7.2.1.2 defines the rules for matching key version numbers. For clarification purposes a paragraph shall be added to requirement 7.2.1.2, defining the rules for selection of key version numbers:</p> <p style="padding-left: 40px;">7.2.1.2 The PIN Pad must verify that one of the public key version numbers ($VKP_{CA, PP}$) listed in the Get Key Check Value Command (to be used by the PSAM to verify the PIN Pad certificates) corresponds to the version number of the public key that created the highest level certificate in a public key certificate chain available to the PIN Pad.</p> <p style="padding-left: 40px;"><i>From the intersection of $VKP_{CA, PP}$'s supported by both the PSAM and the PIN-pad, the PIN-pad shall select the version of $VKP_{CA, PP}$ characterized by the lowest value of the $VKP_{CA, PP}$ key version.</i></p> <p>If there is not match then an error response must be returned with the appropriate response code.</p>
5	2001-11-06	Section 7.2.4 (page 74)	<p>Correction</p> <p>The reference mentioned in requirement 7.2.4.2, step 5 shall be corrected:</p> <p style="padding-left: 40px;">Apply the Padding function defined in section 14.6.7 14.6.8 to</p>
6	2001-11-06	Section 7.2.1 (page 68)	<p>Addition/Clarification</p> <p>A new requirement (7.2.1.5) shall be added in section 7.2.1, to describe the rules for establishing synchronization between PSAM and PIN-pad.</p> <p style="padding-left: 40px;">7.2.1.5 <i>To enable the synchronize process to continue, the response to Get Key Check Value command shall include all data elements as defined in Table 59, even though the Response Code is 'FF80'</i></p>

Item	Date Added	Specification References	Description
7	2004-03-12	Section 8.1 (page 88)	<p>Addition</p> <p>In the existing section 8.1.1 the "Get Amount" command is defined and described.</p> <p>A new section shall be added (between the existing sections 8.1.1 and 8.1.2) to describe the new command "<i>Get Amount 2</i>".</p> <p>The new section (named temporary "8.1.x - Get Amount 2") is described in details on the last pages of the present document.</p> <p>Please refer to the last pages for more information.</p>

Additional information to item number 7 (1)

Get Amount 2

The Get Amount 2 may be used as an alternative to the command Get Amount.

Get Amount 2 may allow transfer of more data elements in both the command and response, compared to Get Amount.

Whether Get Amount or Get Amount 2 shall be used may depend on the actual implementation.

- 8.1.x.1 The Get Amount 2 command must conform to the format defined in Table x1.

Table x1: Get Amount 2 command

Field	Value	Length
Destination Address	'0300' or '0400'	2
Source Address	Any	2
Message Type	'80'	1
ID _{THREAD}	Thread Identifier assigned by the MAD-Handler	1
L _{DATA}	'000B' or '0013' + Length of Discretionary Data	2
Timer Flag	'00' = Not Timed '80' = Timed	1
Time	Time-out value in milliseconds	4
Display Message Code	Code indicating the message to be displayed (see Table 169) '00' indicates that no message is to be displayed.	1
CURR	Currency Code and exponent	3
LEN _{DD}	Length of Discretionary Data	2
Discretionay Data	Discretionary Data	variable
SP _{MAC}	If Destination Address is '0300', MAC included. MAC on preceding data elements [Destination Address – Discretionary Data], computed using KSES _{MAC} .	0 or 8

Additional information to item number 7 (2)

The contents of the data element Discretionary Data is implementation specific.

The definition of Discretionary Data may be different for command and response.

Discretionary Data included in the command may e.g. define data relevant for the calculation of the Transaction Amount returned in the response.

Discretionary Data included in the response may define additional data relevant for the subsequent transaction processing.

- 8.1.x.2 The Get Amount response must conform to the format defined in Table x2.
- 8.1.x.3 If the currency code and exponent in the command were zeros, then the Merchant Application Handler must return the currency of the amount in the response.
- 8.1.x.4 If the merchant application must display a message to the merchant or the user for amount entry, the Display Message Code indicates the message to be displayed.
- 8.1.x.5 If the Merchant Application does not use a display to request an amount entry, and the command issued contained a Display Message Code, but the amount was still successfully entered, the Response Code 'successfully processed' must only be returned in the case where the merchant application automatically replies to the command (for example, in a vending machine).
- 8.1.x.6 If a display is used in the Get Amount process and the Merchant Application Handler does not recognize the Display Message Code, a Response Code 'FF34' must be returned. In this case the amount returned, if any, is not reliable.

Additional information to item number 7 (3)

Table x2: Response to Get Amount 2 command

Field	Value	Length
Destination Address	Any	2
Source Address	'0300' or '0400'	2
Message Type	'FF'	1
ID _{THREAD}	Thread Identifier of the request	1
L _{DATA}	'000B' or '0013' + Length of Discretionary Data	2
Transaction Amount	Transaction Amount	4
CURR	Currency Code and exponent	3
LEN _{DD}	Length of Discretionary Data	2
Discretionay Data	Discretionary Data	variable
SP _{MAC}	If Source Address is '0300', MAC included. MAC on preceding data elements [Transaction Amount – Discretionary Data] SP _{MAC} (from the command), computed using KSES _{MAC} .	0 or 8
Response Code	Response Code	2

8.1.x.7 The Response Codes applicable to the Get Amount 2 command are defined in Table x3.

Additional information to item number 7 (4)

Table x3: Response Codes to Get Amount command

Response Code	Description
'FF34'	Unknown Message Code
'FF40'	Invalid Currency
'FF41'	Invalid Currency Exponent
'FFF2'	<i>Time-out</i> : the requested operation is valid, but some external event necessary for the proper execution failed to arrive in time.
'FFF3'	<i>Handler Error</i> : generic message that an unspecified error has occurred.
'FFF5'	<i>Handler busy</i> : the Handler received the message but is unable to process it at this moment. The requesting Handler must try again later
'FFF6'	<i>Insufficient resources</i> : the requested operation is valid, but insufficient resources exist to successfully execute the requested function.
'FFF7'	<i>Handler must be opened</i> : the Handler is not in <i>open</i> status and therefore cannot perform the requested action.
'FFFB'	<i>Unsupported operation</i> : the Handler has received a command or an associated data set that was unrecognized or unsupported.