



***Technical Reference Guide –  
Open Terminal  
Requirement Specification  
2006–07–01***

# How to Contact PBS A/S

PBS A/S  
Lautrupbjerg 10  
DK-2750 Ballerup  
DENMARK

Tel.no.: +45 44 68 44 68, att. PE 862 Chip og Terminaler  
Fax.no.: +45 44 86 09 30  
E-mail: pe.862@pbs.dk  
Web-site: www.pbs.dk

## Disclaimers

### Copyright Information

This document contains information proprietary to PBS 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 PBS 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 PBS 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 PBS A/S.

### Trademarks

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

### Limitation of Liability

Under no circumstances shall PBS 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 PBS 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 type of Terminal must be certified by PBS A/S before being installed at Merchant locations and being prepared for transmission of transactions to PBS A/S.

# 0. Table of Contents

## 0.1 List of Sections

	page
<b>0. Table of Contents</b> .....	<b>0–1</b>
<b>0.1 List of Sections</b> .....	<b>0–1</b>
<b>1. Revision Log</b> .....	<b>1–1</b>
<b>2. Object and Field of Application</b> .....	<b>2–1</b>
<b>2.1 Target Group</b> .....	<b>2–1</b>
<b>2.2 Objectives</b> .....	<b>2–1</b>
<b>2.3 Scope</b> .....	<b>2–1</b>
<b>2.4 Level of Detail</b> .....	<b>2–2</b>
<b>2.5 Document Structure</b> .....	<b>2–3</b>
<b>3. Definitions</b> .....	<b>3–1</b>
<b>3.1 Introduction</b> .....	<b>3–1</b>
<b>3.2 Terminology</b> .....	<b>3–1</b>
<b>3.2.1 Abbreviations</b> .....	<b>3–1</b>
<b>3.2.2 Terms</b> .....	<b>3–3</b>
<b>3.2.3 Notation</b> .....	<b>3–4</b>
<b>3.3 Requirement Numbering</b> .....	<b>3–6</b>
<b>3.4 References</b> .....	<b>3–7</b>
<b>3.5 Bibliography</b> .....	<b>3–11</b>
<b>3.6 Related Websites</b> .....	<b>3–11</b>
<b>4. System Overview</b> .....	<b>4–1</b>
<b>4.1 Introduction</b> .....	<b>4–1</b>
<b>4.2 Background</b> .....	<b>4–2</b>
<b>4.2.1 History</b> .....	<b>4–2</b>
<b>4.2.2 Standards</b> .....	<b>4–2</b>
<b>4.2.3 Technology</b> .....	<b>4–4</b>
<b>4.2.4 Danish Regulations</b> .....	<b>4–5</b>
<b>4.2.5 Operational Regulations</b> .....	<b>4–6</b>
<b>4.3 Business Requirements</b> .....	<b>4–6</b>
<b>4.3.1 Major Requirements</b> .....	<b>4–6</b>
<b>4.4 Terminal Types</b> .....	<b>4–7</b>
<b>4.4.1 Terminal Environments, Debit/Credit</b> .....	<b>4–9</b>
<b>4.5 Terminal Model</b> .....	<b>4–11</b>
<b>4.5.1 Terminal Architecture for PSAM Applications (TAPA)</b> .....	<b>4–11</b>
<b>4.5.2 A Physical Implementation of the TAPA Model</b> .....	<b>4–13</b>
<b>4.5.3 Application Selection</b> .....	<b>4–18</b>

	<b>page</b>
<b>4.6 Transaction Types</b> .....	<b>4-19</b>
<b>4.6.1 Card Related Transactions for the Debit/Credit Application</b> .....	<b>4-19</b>
<b>4.6.2 Administrative Processes for the Debit/Credit Application</b> .....	<b>4-21</b>
<b>4.6.3 Transaction and Message Flow, Debit/Credit</b> .....	<b>4-22</b>
<b>4.7 Security</b> .....	<b>4-24</b>
<b>4.7.1 Security Zones, Debit/Credit</b> .....	<b>4-24</b>
<b>4.8 Developing an OTRS Terminal</b> .....	<b>4-25</b>
<b>4.8.1 Development Phases</b> .....	<b>4-26</b>
<b>4.8.2 Certification of Terminals, PEDs, and Environment</b> .....	<b>4-26</b>
<b>5. Application-independent Requirements</b> .....	<b>5-1</b>
<b>5.1 Introduction</b> .....	<b>5-1</b>
<b>5.1.1 Terminal Profiles</b> .....	<b>5-1</b>
<b>5.1.2 Related Specifications</b> .....	<b>5-1</b>
<b>5.1.3 Documentation</b> .....	<b>5-2</b>
<b>5.1.4 Patent Issues</b> .....	<b>5-2</b>
<b>5.2 General Requirements</b> .....	<b>5-3</b>
<b>5.2.1 Protected Functions</b> .....	<b>5-3</b>
<b>5.2.2 Protected Functions – Manufacturer Specific Functions</b> .....	<b>5-3</b>
<b>5.3 The Router</b> .....	<b>5-4</b>
<b>5.3.1 Functional Requirements</b> .....	<b>5-4</b>
<b>5.3.2 Exception Handling</b> .....	<b>5-4</b>
<b>5.3.3 Command Flow</b> .....	<b>5-4</b>
<b>5.4 Multi-Application Driver Handler (MAD-Handler)</b> .....	<b>5-4</b>
<b>5.4.1 General Requirements</b> .....	<b>5-4</b>
<b>5.4.2 Printing</b> .....	<b>5-5</b>
<b>5.4.3 Log</b> .....	<b>5-5</b>
<b>5.4.4 Exception Handling</b> .....	<b>5-6</b>
<b>5.5 Card Handler</b> .....	<b>5-7</b>
<b>5.5.1 General Requirements</b> .....	<b>5-7</b>
<b>5.5.2 Sub-handler, Magnetic Stripe Card Reader (MSCR)</b> .....	<b>5-8</b>
<b>5.5.3 Sub-handler, ICCR – General</b> .....	<b>5-9</b>
<b>5.5.4 Sub-handler, ICCR – Processor Card Reader</b> .....	<b>5-10</b>
<b>5.5.5 Interface to the Processor Card</b> .....	<b>5-11</b>
<b>5.6 User Interface Handler</b> .....	<b>5-11</b>
<b>5.6.1 Sub-handler, PIN Pad</b> .....	<b>5-11</b>
<b>5.6.2 Sub-handler, Printer</b> .....	<b>5-14</b>
<b>5.6.3 Sub-handler, Cardholder Key Pad</b> .....	<b>5-14</b>
<b>5.6.4 Sub-handler, Cardholder Display</b> .....	<b>5-14</b>
<b>5.6.5 Sub-handler, Audio Indicator</b> .....	<b>5-16</b>
<b>5.7 Merchant Application Handler</b> .....	<b>5-17</b>
<b>5.7.1 Sub-handler, Log</b> .....	<b>5-17</b>
<b>5.7.2 Sub-handler, Serial Ports</b> .....	<b>5-17</b>
<b>5.7.3 Interface between CAD and Merchant Application</b> .....	<b>5-17</b>
<b>5.8 PSAM Handler</b> .....	<b>5-17</b>
<b>5.8.1 Interface to the PSAM</b> .....	<b>5-17</b>
<b>5.8.2 EMV Compatibility of the PSAM Interface</b> .....	<b>5-18</b>
<b>5.8.3 Commands between the CAD and the PSAM</b> .....	<b>5-20</b>
<b>5.9 Data Store Handler</b> .....	<b>5-21</b>
<b>5.9.1 Sub-handler, Data Store</b> .....	<b>5-21</b>

	<b>page</b>
<b>5.10 Communication Handler</b> .....	5–22
<b>5.10.1 General Requirements</b> .....	5–22
<b>5.11 Event Handler</b> .....	5–22
<b>5.11.1 General Requirements</b> .....	5–22
<b>5.12 Terminal Initialization</b> .....	5–22
<b>5.12.1 Reset of the CAD</b> .....	5–22
<b>5.13 Application Selection</b> .....	5–22
<b>5.13.1 Introduction</b> .....	5–22
<b>5.13.2 Building the MSC Selection Table</b> .....	5–23
<b>5.13.3 Building the AID Selection Table (for ICCs)</b> .....	5–25
<b>5.13.4 MSC Application Selection</b> .....	5–27
<b>5.13.5 ICC Application Selection</b> .....	5–28
<b>5.13.6 Combined MSC and ICC Application Selection</b> .....	5–31
<b>5.14 Fallback from Chip (ICC) to Magnetic Stripe (MSC)</b> .....	5–33
<b>5.14.1 Introduction</b> .....	5–33
<b>5.14.2 General Requirements</b> .....	5–33
<b>5.14.3 The role of the PSAM</b> .....	5–35
<b>5.14.4 Final Decision</b> .....	5–36
<b>5.15 Language Selection</b> .....	5–42
<b>5.15.1 General Requirements</b> .....	5–42
<b>5.15.2 ICC Language Selection</b> .....	5–42
<b>6. Debit/Credit Functionality</b> .....	<b>6–1</b>
<b>6.1 Application Initialization</b> .....	<b>6–1</b>
<b>6.1.1 Introduction</b> .....	<b>6–1</b>
<b>6.1.2 Power On</b> .....	<b>6–2</b>
<b>6.1.3 Restart</b> .....	<b>6–6</b>
<b>6.1.4 Installation</b> .....	<b>6–10</b>
<b>6.1.5 New Application Data</b> .....	<b>6–10</b>
<b>6.1.6 Configuration</b> .....	<b>6–11</b>
<b>6.1.7 PSAM/PIN Pad Synchronization</b> .....	<b>6–12</b>
<b>6.1.8 PSAM Shutdown</b> .....	<b>6–14</b>
<b>6.2 Business Calls</b> .....	<b>6–14</b>
<b>6.2.1 Purchase</b> .....	<b>6–14</b>
<b>6.2.2 Original Authorization</b> .....	<b>6–15</b>
<b>6.2.3 Supplementary Authorization</b> .....	<b>6–16</b>
<b>6.2.4 Capture</b> .....	<b>6–17</b>
<b>6.2.5 Reversal (Authorization)</b> .....	<b>6–18</b>
<b>6.2.6 Refund</b> .....	<b>6–19</b>
<b>6.2.7 Business Calls and Terminal Environments</b> .....	<b>6–20</b>
<b>6.3 Gratuity and other surcharges</b> .....	<b>6–20</b>
<b>6.3.1 Purchase &amp; Refund</b> .....	<b>6–21</b>
<b>6.3.2 Token Based Transactions</b> .....	<b>6–21</b>
<b>6.3.3 Gratuity and other Cardholder defined Surcharges</b> .....	<b>6–23</b>
<b>6.3.4 Card related fees and other Merchant Defined Surcharges</b> .....	<b>6–23</b>
<b>6.3.5 Cashback</b> .....	<b>6–24</b>
<b>6.3.6 Validation, Control and Limitations of Surcharges</b> .....	<b>6–24</b>
<b>6.4 Cardholder Verification</b> .....	<b>6–25</b>
<b>6.4.1 PIN Entry</b> .....	<b>6–25</b>
<b>6.4.2 Signature</b> .....	<b>6–26</b>
<b>6.4.3 No CVM</b> .....	<b>6–27</b>

	<b>page</b>
<b>6.5 Tokens</b> .....	6-27
<b>6.5.1 The Use of Tokens</b> .....	6-27
<b>6.6 Multi-Application Driver Handler (MAD-Handler)</b> .....	6-30
<b>6.6.1 Printing</b> .....	6-30
<b>6.7 User Interface Handler</b> .....	6-31
<b>6.7.1 Sub-handler, Cardholder Display</b> .....	6-31
<b>6.7.2 Requirements for PIN Entry State</b> .....	6-35
<b>6.8 Merchant Application Handler</b> .....	6-37
<b>6.8.1 Sub-handler, Printer</b> .....	6-37
<b>6.8.2 Sub-handler, Merchant Display</b> .....	6-37
<b>6.9 Card Related Transactions</b> .....	6-39
<b>6.10 EMV Card Transactions</b> .....	6-40
<b>6.10.1 Transaction Processing</b> .....	6-40
<b>6.10.2 Initialization of the EMV Debit/Credit Payment Transaction</b> .....	6-40
<b>6.10.3 Initiate EMV Payment</b> .....	6-41
<b>6.10.4 EMV Payment</b> .....	6-44
<b>6.10.5 Validate Data</b> .....	6-47
<b>6.10.6 Complete EMV Payment</b> .....	6-49
<b>6.10.7 EMV-related Data Elements</b> .....	6-51
<b>6.11 Optimizing the Transaction Time</b> .....	6-54
<b>6.11.1 Introduction</b> .....	6-54
<b>6.11.2 Accelerated PIN Entry</b> .....	6-54
<b>6.11.3 Release of the ICC</b> .....	6-56
<b>6.12 Magnetic Stripe Card Transactions</b> .....	6-67
<b>6.12.1 Transaction Processing</b> .....	6-67
<b>6.12.2 Initialization of the MSC Debit/Credit Payment Transaction</b> .....	6-67
<b>6.12.3 Initiate MSC Payment</b> .....	6-68
<b>6.12.4 MSC Payment</b> .....	6-70
<b>6.12.5 Validate Data</b> .....	6-73
<b>6.12.6 Complete Payment</b> .....	6-74
<b>6.13 Key Entered Card Transactions</b> .....	6-87
<b>6.13.1 Transaction Processing</b> .....	6-87
<b>6.13.2 Initialization of the Key Entered Debit/Credit Payment Transaction</b> .....	6-87
<b>6.13.3 Initiate Key Entered Payment</b> .....	6-88
<b>6.13.4 Key Entered Payment</b> .....	6-90
<b>6.13.5 Validate Data</b> .....	6-93
<b>6.13.6 Complete Key Entered Payment</b> .....	6-94
<b>6.14 Token based Transactions</b> .....	6-102
<b>6.14.1 Transaction Processing</b> .....	6-102
<b>6.14.2 Initialization of the Token Based Debit/Credit Payment Transaction</b> .....	6-102
<b>6.14.3 Initiate Token Based Payment</b> .....	6-103
<b>6.14.4 Token Based Payment</b> .....	6-105
<b>6.14.5 Validate Data</b> .....	6-107
<b>6.14.6 Complete Token Based Payment</b> .....	6-107
<b>6.15 Addendum Records</b> .....	6-118
<b>6.15.1 Introduction</b> .....	6-118
<b>6.15.2 Handling of Addendum Records</b> .....	6-118
<b>6.16 Administrative Transactions and Processes</b> .....	6-121
<b>6.16.1 Introduction</b> .....	6-121
<b>6.16.2 Installation Transaction</b> .....	6-121
<b>6.16.3 Advice Transfer, Advice Enclosing and Advice Forwarding</b> .....	6-123

	<b>page</b>
6.16.4 Advice Transfer .....	6–128
6.16.5 Advice Enclosing .....	6–131
6.16.6 Advice Forwarding .....	6–132
6.16.7 PSAM Update Transaction .....	6–133
6.16.8 PSAM Deactivation Transaction .....	6–135
6.16.9 Clock Synchronization .....	6–136
6.16.10 Counters and Batch Numbers .....	6–137
<b>6.17 Online Transactions .....</b>	<b>6–139</b>
6.17.1 Advice Request Flag .....	6–139
6.17.2 PSAM Scripts .....	6–139
6.17.3 Repeat Messages .....	6–139
6.17.4 Communication Session .....	6–140
6.17.5 Terminal Operator Communication Access Points .....	6–142
<b>6.18 Exception Handling .....</b>	<b>6–143</b>
6.18.1 Introduction .....	6–143
6.18.2 General Rules .....	6–143
6.18.3 Categories .....	6–145
6.18.4 Terminal Related Errors .....	6–145
6.18.5 PSAM Related Errors .....	6–147
6.18.6 Host Declined Transactions (Requests) .....	6–147
6.18.7 Host Declined Transactions (Advices) .....	6–150
6.18.8 PSAM Declined Online Transactions .....	6–150
6.18.9 PSAM Declined Offline Transactions .....	6–150
6.18.10 Card Declined Transactions .....	6–151
6.18.11 Cardholder Initiated Actions .....	6–151
6.18.12 Communication Statistics and Error Counters .....	6–152
6.18.13 Authorization Advice .....	6–152
6.18.14 Application Status Words .....	6–152
6.18.15 Message Codes .....	6–152
6.18.16 Action Codes .....	6–153
6.18.17 Merchant Initiated Actions .....	6–154
6.18.18 Time-outs .....	6–154
<b>7. Best Practice .....</b>	<b>7–1</b>
7.1 Introduction .....	7–1
7.2 Documentation .....	7–1
7.3 Terminal Categories .....	7–1
7.4 Choice of Business Call .....	7–2
7.5 Refund .....	7–2
7.6 Support of Card Technologies .....	7–3
7.7 ICC Technology and Fallback to Magnetic Stripe .....	7–3
7.8 Service Packs .....	7–4
7.9 Application Selection .....	7–4
7.10 Support of Cardholder Verification Methods .....	7–5
7.11 Temporary Offline Procedure .....	7–6
7.12 Voice Authorization Calls .....	7–7
7.13 Stop List .....	7–8
7.14 Optimizing the Transaction Time .....	7–8
7.14.1 Parallel Processing .....	7–8
7.14.2 Data Transmission .....	7–9

	<b>page</b>
7.15 Signature Verification and Accept .....	7-10
7.16 Receipts .....	7-11
7.17 Get Amount 2 .....	7-12
7.18 Get Amount 3 .....	7-12
7.19 Transaction Result .....	7-13
7.20 Transaction Checks .....	7-13
7.21 Log and Totals .....	7-14
7.22 Merchant Application Log .....	7-15
7.23 Cashback Amount .....	7-15
7.24 Addition of Surcharges and Fees .....	7-16
7.25 Gratuity .....	7-16
7.26 Dual Communication Access Points .....	7-17
7.27 Automatic Advice Transfer if no Customers being Serviced .....	7-17
7.28 Host Messages .....	7-18
7.29 Transaction State Information .....	7-19
7.30 Local PIN .....	7-19
7.31 Certification .....	7-19
7.32 Cash/Quasi-Cash Terminals .....	7-20
7.33 POS Terminal/CAT Levels vs. Terminal Type .....	7-21
<b>8. Commands and Responses .....</b>	<b>8-1</b>
8.1 Introduction .....	8-1
8.2 Command Overview .....	8-2
8.3 Error Responses .....	8-8
8.3.1 MAD-Handler Interface to the PSAM .....	8-8
8.4 Commands used during Initialization .....	8-9
8.4.1 Start-up PSAM .....	8-9
8.4.2 Get Supported AIDs .....	8-10
8.4.3 Get MSC Table .....	8-12
8.4.4 Get Debit/Credit File Characteristics .....	8-14
8.4.5 Configure PSAM Application .....	8-16
8.4.6 Synchronize PSAM/PIN Pad .....	8-17
8.4.7 Get Next .....	8-18
8.4.8 Exchange Debit/Credit Static Information .....	8-19
8.5 Debit/Credit Administrative Commands .....	8-21
8.5.1 Install .....	8-21
8.5.2 Validate Install Data .....	8-22
8.5.3 Add Addendum Record .....	8-24
8.5.4 Deactivate PSAM .....	8-25
8.5.5 Create Service Record .....	8-26
8.5.6 Get Debit/Credit Properties .....	8-28
8.5.7 Set Debit/Credit Properties .....	8-32
8.5.8 PSAM Update .....	8-34
8.6 Debit/Credit Transaction Commands .....	8-35
8.6.1 Initiate EMV Payment .....	8-35
8.6.2 Initiate EMV Payment 2 .....	8-37
8.6.3 EMV Payment .....	8-40
8.6.4 Validate Data .....	8-41



	<b>page</b>
8.6.5	Validate Data 2 ..... 8–44
8.6.6	Complete Payment ..... 8–48
8.6.7	Initiate MSC Payment ..... 8–49
8.6.8	Initiate MSC Payment 2 ..... 8–51
8.6.9	MSC Payment ..... 8–54
8.6.10	Complete Payment ..... 8–56
8.6.11	Initiate Key Entered Payment ..... 8–57
8.6.12	Key Entered Payment ..... 8–60
8.6.13	Complete Payment ..... 8–62
8.6.14	Initiate Token Based Payment ..... 8–64
8.6.15	Initiate Token Based Payment 2 ..... 8–65
8.6.16	Token Based Payment ..... 8–68
8.6.17	Complete Payment ..... 8–70
8.6.18	Check Stop List ..... 8–71
8.6.19	Verify Signature ..... 8–72
8.6.20	Get Merchant Data ..... 8–74
8.6.21	Transaction State Information ..... 8–76
8.6.22	Repeat Last ICC Response ..... 8–79
8.6.23	Get Amount ..... 8–80
8.6.24	Get Amount 2 ..... 8–82
8.6.25	Get Amount 3 ..... 8–84
8.7	Local PIN Commands ..... 8–86
8.7.1	Load LP Keys Command – Method Number 1 ..... 8–86
8.7.2	Local PIN Validation ..... 8–87
8.8	ASW1–ASW2 Coding ..... 8–92
8.8.1	Application Specific ASW1–ASW2 Coding (Debit/Credit) ..... 8–93
8.8.2	ASW1–ASW2 Applicable for Local PIN ..... 8–138
<b>9.</b>	<b>Data Elements ..... 9–1</b>
9.1	Introduction ..... 9–1
9.1.1	Coding of Data Elements ..... 9–1
9.1.2	Data Elements Defined in EMV and TAPA ..... 9–1
9.2	Data Elements for the Debit/Credit Application ..... 9–2
9.2.1	Account Type ..... 9–2
9.2.2	Action Code ..... 9–2
9.2.3	Addendum Record ..... 9–2
9.2.4	AID (Application Identifier) ..... 9–3
9.2.5	ALGVLP ..... 9–3
9.2.6	Amount ..... 9–3
9.2.7	Amount, Other ..... 9–3
9.2.8	Amount Request ..... 9–3
9.2.9	Amount Status ..... 9–4
9.2.10	Application Label ..... 9–4
9.2.11	Approval Code ..... 9–4
9.2.12	ASI (Application Selection Indicator) ..... 9–4
9.2.13	Batch Number ..... 9–4
9.2.14	Card Data ..... 9–5
9.2.15	Card Data Source ..... 9–5
9.2.16	Card Name ..... 9–5
9.2.17	Card Sequence Number ..... 9–5
9.2.18	Card Service Info ..... 9–5
9.2.19	CNT <sub>X</sub> (Count of X) ..... 9–6
9.2.20	CURR <sub>C</sub> (Currency Code) ..... 9–6

	<b>page</b>
9.2.21	<b>CURRE</b> (Currency Exponent) . . . . . 9-6
9.2.22	<b>CV-2</b> (Card Verification, method 2) . . . . . 9-6
9.2.23	<b>CVM Status</b> . . . . . 9-7
9.2.24	<b>Data Requested</b> . . . . . 9-7
9.2.25	<b>Duplicate Transaction Time-out</b> . . . . . 9-8
9.2.26	<b>EMV Checksum</b> . . . . . 9-8
9.2.27	<b>Expiry Date</b> . . . . . 9-8
9.2.28	<b>FILEIDADMIN</b> . . . . . 9-8
9.2.29	<b>FILEIDPRIORITY,n</b> . . . . . 9-8
9.2.30	<b>Hardware Version Number</b> . . . . . 9-9
9.2.31	<b>Host Request</b> . . . . . 9-9
9.2.32	<b>Host Response</b> . . . . . 9-9
9.2.33	<b>IDPSAM</b> (Identifier for a PSAM) . . . . . 9-9
9.2.34	<b>IDPSAMAPP</b> (TAPA PSAM Application Identifier) . . . . . 9-9
9.2.35	<b>IDPSAMCREATOR</b> . . . . . 9-9
9.2.36	<b>IDPSAMCREATOR</b> . . . . . 9-9
9.2.37	<b>Info Level</b> . . . . . 9-10
9.2.38	<b>Issuer DD</b> (Issuer Discretionary Data in FCI) . . . . . 9-10
9.2.39	<b>Issuer Envelope Data</b> . . . . . 9-10
9.2.40	<b>Key Check Value (KCV)</b> . . . . . 9-10
9.2.41	<b>LEN<sub>X</sub></b> (Length of Field X) . . . . . 9-11
9.2.42	<b>Local PIN Verification Status</b> . . . . . 9-11
9.2.43	<b>Magnetic Stripe Contents</b> . . . . . 9-11
9.2.44	<b>MAD-Handler ID</b> . . . . . 9-11
9.2.45	<b>MDOL</b> (MAD-Handler Data Object List) . . . . . 9-11
9.2.46	<b>MDOL Data</b> . . . . . 9-12
9.2.47	<b>MEADDRESS</b> (Merchant Address) . . . . . 9-12
9.2.48	<b>MEBRN</b> (Business Registration Number) . . . . . 9-12
9.2.49	<b>MECITY</b> (Merchant City Name) . . . . . 9-12
9.2.50	<b>ME<sub>NAME</sub></b> (Merchant Name) . . . . . 9-12
9.2.51	<b>ME<sub>NUMBER</sub></b> (Merchant Number) . . . . . 9-12
9.2.52	<b>ME<sub>PHONE</sub></b> (Merchant Phone No.) . . . . . 9-13
9.2.53	<b>ME<sub>ZIP</sub></b> (Merchant Postal Code) . . . . . 9-13
9.2.54	<b>MI</b> (Merchant Initiative) . . . . . 9-13
9.2.55	<b>MTI</b> (Message Type Identifier) . . . . . 9-14
9.2.56	<b>MTI of the Original Message</b> . . . . . 9-15
9.2.57	<b>PAN</b> (Primary Account Number) . . . . . 9-15
9.2.58	<b>PAN Sequence Number</b> . . . . . 9-15
9.2.59	<b>PAN<sub>FROM</sub></b> . . . . . 9-15
9.2.60	<b>PAN<sub>TO</sub></b> . . . . . 9-15
9.2.61	<b>PIN Data</b> . . . . . 9-15
9.2.62	<b>POS Capability Code</b> . . . . . 9-16
9.2.63	<b>POS Entry Mode</b> . . . . . 9-16
9.2.64	<b>PSAM Code Checksum</b> . . . . . 9-16
9.2.65	<b>PSAM Config Checksum</b> . . . . . 9-16
9.2.66	<b>PSAM D/C Life Cycle State</b> . . . . . 9-17
9.2.67	<b>PSAM Subversion</b> . . . . . 9-17
9.2.68	<b>PSAM Version</b> . . . . . 9-17
9.2.69	<b>Reference STAN</b> . . . . . 9-17
9.2.70	<b>RID<sub>PSAM</sub></b> . . . . . 9-17
9.2.71	<b>Service Code</b> . . . . . 9-18
9.2.72	<b>Service Packs Supported</b> . . . . . 9-18
9.2.73	<b>Signature Verification</b> . . . . . 9-18
9.2.74	<b>Software Version Number</b> . . . . . 9-18

	<b>page</b>
9.2.75 STAN (System Trace Audit Number) .....	9–19
9.2.76 Statistics .....	9–19
9.2.77 Stop List Status .....	9–19
9.2.78 Terminal Approval No. ....	9–19
9.2.79 Terminal Checksum .....	9–20
9.2.80 Terminal Identification .....	9–20
9.2.81 Terminal Manufacturer ID .....	9–20
9.2.82 Terminal Serial Number .....	9–20
9.2.83 Terminal Settings .....	9–20
9.2.84 Token .....	9–21
9.2.85 TRACK2 DATA .....	9–21
9.2.86 Transaction Category Code .....	9–21
9.2.87 Transaction Gratuity Amount .....	9–21
9.2.88 Transaction Request (TR) .....	9–22
9.2.89 Transaction State Information .....	9–22
9.2.90 Transaction Status .....	9–23
9.2.91 Transaction Total Amount .....	9–23
9.2.92 Transaction Type (TT) .....	9–23
9.2.93 Type of Application .....	9–23
9.2.94 Update Data .....	9–24
9.2.95 Update Number .....	9–24
<b>9.3 Data Elements specific for the Local PIN Application .....</b>	<b>9–25</b>
9.3.1 Key Check Value (KCV) .....	9–25
9.3.2 Last PIN incorrect .....	9–25
9.3.3 LP-KEK .....	9–25
9.3.4 LP-KEK-Version .....	9–25
9.3.5 LP-Key .....	9–25
9.3.6 LP-Key-Chain .....	9–26
9.3.7 LP-Key-Version .....	9–26
9.3.8 Maximum PIN digits .....	9–26
9.3.9 Method Number .....	9–26
9.3.10 Minimum PIN digits .....	9–26
9.3.11 Number of PIN tries left .....	9–26
9.3.12 Time .....	9–27
9.3.13 Timer Flag .....	9–27
9.3.14 Transaction Counter .....	9–27
<b>10. Design Requirements .....</b>	<b>10–1</b>
10.1 General Considerations .....	10–1
10.1.1 Environmental Requirements .....	10–1
10.1.2 Requirements from Third Parties .....	10–2
10.1.3 Documentation .....	10–2
10.1.4 Marking .....	10–3
10.1.5 Servicing the Terminal .....	10–4
10.2 Mechanical Design .....	10–4
10.2.1 General Requirements .....	10–4
10.2.2 Combined Card Reader .....	10–6
10.2.3 Integrated Circuit Card Reader .....	10–6
10.2.4 Magnetic Stripe Card Reader .....	10–7
10.2.5 PSAM Card Reader(s) .....	10–8
10.2.6 Merchant Application Interface .....	10–8
10.2.7 Visual Indicators .....	10–9
10.2.8 Audio Indicator .....	10–10

	<b>page</b>
10.2.9 Cardholder Keyboard / Command Keys .....	10-11
10.2.10 PIN Pad .....	10-11
10.2.11 Receipt Printer .....	10-16
<b>10.3 Electrical Design .....</b>	<b>10-16</b>
10.3.1 Introduction .....	10-16
10.3.2 General Requirements .....	10-17
10.3.3 Electrical Safety .....	10-17
10.3.4 Electromagnetic Compatibility .....	10-17
10.3.5 Circuit Design .....	10-17
10.3.6 Electrical Interfaces .....	10-18
10.3.7 Data Store .....	10-20
<b>10.4 Software Design .....</b>	<b>10-20</b>
10.4.1 Introduction .....	10-20
10.4.2 General Requirements .....	10-20
10.4.3 Additional Requirements to the PED Software .....	10-21
10.4.4 Data Management .....	10-24
10.4.5 Storage of Data .....	10-24
10.4.6 Storage of Software .....	10-25
10.4.7 Download Requirements .....	10-25
<b>10.5 Network Design .....</b>	<b>10-27</b>
10.5.1 Integration Between Terminal and Cash Register .....	10-27
10.5.2 Network Connection .....	10-27
10.5.3 One Terminal Integrated with Several Cash Registers .....	10-28
<b>11. Service Packs .....</b>	<b>11-1</b>
11.1 Introduction .....	11-1
11.2 Selection of Service Packs supported .....	11-1
11.2.1 Terminal – Terminal Approval No. ....	11-1
11.3 Service Packs Overview .....	11-2
11.4 Service Pack No. 1 .....	11-2
11.4.1 MSC PIN Retry .....	11-3
11.4.2 Get Amount 2 .....	11-3
11.4.3 Validate Data 2 .....	11-4
11.5 Service Pack No. 2 .....	11-5
11.5.1 Get Amount 3 .....	11-5
11.5.2 Message Size .....	11-6
11.5.3 Issuer Envelope Functionality .....	11-7
11.5.4 Initiate Payment 2 / Account Type .....	11-8
<b>Attachment A. Magnetic Stripe Formats .....</b>	<b>A-1</b>
A.1 Introduction .....	A-1
A.1.1 Track 2 Structure .....	A-1
A.2 Credit/Debit Cards .....	A-2
<b>Attachment B. Validation of the PAN (Primary Account Number) .....</b>	<b>B-1</b>
B.1 Check Digit Modulus 10 .....	B-1
B.1.1 Modulus 10 Calculation .....	B-1
B.1.2 Luhn Formula for Calculating Modulus 10 Check Digit .....	B-1
B.1.3 Modulus 10 check digit verification .....	B-2

	page
<b>Attachment C. SDL Notation</b> .....	<b>C–1</b>
<b>C.1 Introduction</b> .....	<b>C–1</b>
<b>C.2 Symbols and their Meaning</b> .....	<b>C–1</b>
<b>Attachment D. Certification</b> .....	<b>D–1</b>
<b>Attachment E. Cardholder Activated Terminals</b> .....	<b>E–1</b>
<b>E.1 Introduction</b> .....	<b>E–1</b>
<b>E.2 CAT Levels</b> .....	<b>E–1</b>
<b>E.2.1 CAT Level 1 – Automated Dispensing Machines</b> .....	<b>E–2</b>
<b>E.2.2 CAT Level 2 – Self–Service Terminals</b> .....	<b>E–2</b>
<b>E.2.3 CAT Level 3 – Limited–Amount Terminals</b> .....	<b>E–2</b>
<b>E.2.4 CAT Level 4 – In–Flight Terminals</b> .....	<b>E–2</b>
<b>Attachment F. Host Communication for the Debit/Credit Application</b> <b>– Protocols and Formats</b> .....	<b>F–1</b>
<b>F.1 Introduction</b> .....	<b>F–1</b>
<b>F.2 General</b> .....	<b>F–1</b>
<b>F.3 Communication Protocols</b> .....	<b>F–1</b>
<b>F.3.1 Physical Layer</b> .....	<b>F–2</b>
<b>F.3.2 Data Link Layer</b> .....	<b>F–3</b>
<b>F.3.3 Network Layer</b> .....	<b>F–3</b>
<b>F.3.4 Transport Layer</b> .....	<b>F–3</b>
<b>F.3.5 Session Layer</b> .....	<b>F–3</b>
<b>F.3.6 Presentation and Application Layers</b> .....	<b>F–3</b>
<b>F.4 Transmission Flows</b> .....	<b>F–3</b>
<b>F.5 Transmission Formats</b> .....	<b>F–4</b>
<b>F.5.1 APACS Message Types</b> .....	<b>F–4</b>
<b>F.5.2 APACS Message Header</b> .....	<b>F–4</b>
<b>F.6 Communication Statistics and Error Counters</b> .....	<b>F–11</b>
<b>F.6.1 Introduction</b> .....	<b>F–11</b>
<b>F.6.2 Communication Interface Statistics</b> .....	<b>F–11</b>
<b>F.6.3 Error Counters</b> .....	<b>F–12</b>
<b>F.6.4 Error Counters, tag TE, TF, TG and TH</b> .....	<b>F–12</b>
<b>F.7 Primitive Data Objects for the APACS Header</b> .....	<b>F–14</b>
<b>F.7.1 Coding of Tag ‘C0’ (Length of APACS 60 Message)</b> .....	<b>F–14</b>
<b>F.7.2 Coding of Tag ‘C1’ (Message Type Identifier)</b> .....	<b>F–14</b>
<b>F.7.3 Coding of Tag ‘C2’ (Function Code)</b> .....	<b>F–14</b>
<b>F.7.4 Coding of Tag ‘C3’ (PSAM Identifier)</b> .....	<b>F–14</b>
<b>F.7.5 Coding of Tag ‘C4’ (Systems Trace Audit Number)</b> .....	<b>F–14</b>
<b>F.7.6 Coding of Tag ‘C5’ (KEK<sub>DATA</sub>)</b> .....	<b>F–14</b>
<b>F.7.7 Coding of Tag ‘C6’ ([KSES<sub>DATA</sub>])</b> .....	<b>F–14</b>
<b>F.7.8 Coding of Tag ‘C7’ (APACS MAC Key Version)</b> .....	<b>F–14</b>
<b>F.7.9 Coding of Tag ‘C8’ (Advice Window Size)</b> .....	<b>F–15</b>
<b>F.7.10 Coding of Tag ‘C9’ (Advice Request Flag)</b> .....	<b>F–15</b>
<b>F.7.11 Coding of Tag ‘CA’ (Display Line for Host Message)</b> .....	<b>F–15</b>
<b>F.7.12 Coding of Tag ‘CB’ (Network Connection Type)</b> .....	<b>F–15</b>
<b>F.7.13 Coding of Tag ‘CC’ (MAD–Handler ID)</b> .....	<b>F–16</b>
<b>F.7.14 Coding of Tag ‘CD’ (Terminal Identification)</b> .....	<b>F–16</b>
<b>F.7.15 Coding of Tag ‘CE’ (Proprietary Data)</b> .....	<b>F–16</b>

	<b>page</b>
F.7.16 Coding of Tag ‘CF’ (Communication Interface Statistics) .....	F-16
F.7.17 Coding of Tag ‘D1’ (Reference STAN) .....	F-17
F.7.18 Coding of Tag ‘D2’ (MTI of the Original Message) .....	F-17
<b>F.8 Detailed Message Formats .....</b>	<b>F-19</b>
F.8.1 Authorization Request Messages (0106/0116) .....	F-20
F.8.2 Authorization Advice Messages (0126/0136) .....	F-26
F.8.3 Financial Request Messages (0206/0216) .....	F-32
F.8.4 Financial Advice Messages (0226/0236) .....	F-38
F.8.5 PSAM Update Messages (0360/0370) .....	F-46
F.8.6 Reversal Advice Messages (0426/0436) .....	F-48
F.8.7 Addendum Record Messages (0624/0634) .....	F-56
F.8.8 Service Record Messages (0624/0634) .....	F-57
F.8.9 Clock Synchronization Messages (0804/0814) .....	F-58
F.8.10 Installation Messages (0804/0814) .....	F-59
F.8.11 Advice Transfer Messages (0804/0814) .....	F-60
F.8.12 PSAM Update Messages (0804/0814/0844) .....	F-61
F.8.13 PSAM Deactivation Messages (0804/0814) .....	F-62
<b>F.9 Coding of Application Specific Fields .....</b>	<b>F-63</b>
F.9.1 Coding Conventions .....	F-63
F.9.2 Coding of Field 3 (Processing Code) .....	F-63
F.9.3 Coding of Field 15 (GMT Offset) .....	F-64
F.9.4 Coding of Field 21 (POS Capability Code) .....	F-64
F.9.5 Coding of Field 22 (POS Entry Mode) .....	F-67
F.9.6 Coding of Field 24 (Function Code) .....	F-74
F.9.7 Coding of Field 25 (Message Reason Code) .....	F-75
F.9.8 Coding of Field 27 (Download Control) .....	F-76
F.9.9 Coding of Field 39 (Action Code) .....	F-76
F.9.10 TLV Coding of Field 44 (Additional Response Data) .....	F-80
F.9.11 TLV Coding of Field 46 (CAD Management/Service Quality Data) .....	F-81
F.9.12 Coding of Field 47 (Additional Data – National) .....	F-83
F.9.13 Coding of Field 55 (ICC System Related Data) .....	F-84
F.9.14 Coding of Field 56 (Original Data Elements) .....	F-85
F.9.15 Coding of Field 60 (PSAM Identifier) .....	F-85
F.9.16 Coding of Field 61 (Random Number) .....	F-86
F.9.17 Coding of Field 62 (Merchant Initiative) .....	F-86
F.9.18 TLV Coding of Field 63 (PSAM Updates) .....	F-86
F.9.19 Coding of Field 71 (Message Number) .....	F-86
F.9.20 TLV Coding of Field 72 (Addendum Record) .....	F-87
<b>Attachment G. Receipts .....</b>	<b>G-1</b>
<b>G.1 Receipts .....</b>	<b>G-1</b>
G.1.1 General Requirements .....	G-1
G.1.2 General Layout for Receipts .....	G-3
<b>G.2 Receipt Variants .....</b>	<b>G-9</b>
G.2.1 General Requirements .....	G-9
G.2.2 Receipt for Declined Transaction .....	G-12
G.2.3 Receipt for Failed Transaction .....	G-12
G.2.4 Receipt for Rejected Signature .....	G-13
G.2.5 Original Authorization .....	G-13
G.2.6 Reversal (Authorization) .....	G-15
G.2.7 Transaction Stopped/Canceled .....	G-16
G.2.8 Receipts without Carbon Copy with Signature as CVM .....	G-17
G.2.9 Receipts with Carbon Copy and Signature as CVM .....	G-18

	<b>page</b>
G.2.10 Additional Information Concerning EURO Currency .....	G–19
G.2.11 Cashback, Additional Fees etc. ....	G–19
G.2.12 Manual Cash Disbursement .....	G–21
G.3 Printing of PAN and Transaction Condition Codes .....	G–23
G.3.1 Truncation of the PAN .....	G–23
G.3.2 Transaction Condition Codes .....	G–24
G.4 Additional Receipts for logging Purposes .....	G–25
G.4.1 Introduction .....	G–25
G.4.2 Signature based Transactions .....	G–26
G.4.3 Refund Transactions .....	G–26
G.4.4 PIN– and No–CVM based Transactions .....	G–26
G.5 Receipts printed, depending on Business Environment and actual CVM .....	G–27
G.5.1 PIN or No CVM .....	G–30
G.5.2 Signature or Combined CVM (both PIN and Signature used) .....	G–31
G.5.3 Refund (Signature) .....	G–33
G.5.4 Signature or Combined CVM – Possibility for adding Extra Amount .....	G–35
G.5.5 Signature or Combined CVM – after adding Extra Amount .....	G–37
G.5.6 Original Authorization with PIN or Combined CVM .....	G–39
G.5.7 Release of Token – Reversal (Authorization) .....	G–40
G.5.8 PIN or No CVM – Extra Amount added before Cardholder Acceptance .....	G–41
G.5.9 Signature or Combined CVM – Extra Amount added before Cardholder Acceptance .....	G–42
G.6 Receipts – 18 Characters per Line .....	G–44
G.6.1 General Requirements .....	G–44
G.6.2 Standard Layout – 24 Characters per Line .....	G–45
G.6.3 Standard Layout – 18 Characters per Line .....	G–46
G.6.4 Purchase – Based on PIN or No CVM (18 Characters per Line) .....	G–47
G.6.5 Purchase – Based on Signature or Combined CVM (18 Characters per Line) ..	G–48
G.6.6 Refund – Based on Signature (18 Characters per Line) .....	G–50
G.7 Receipts in English .....	G–52
G.7.1 General Requirements .....	G–52
<b>Attachment H. Privacy Shield on PIN Entry Devices .....</b>	<b>H–1</b>
H.1 Introduction .....	H–1
H.1.1 Terminology .....	H–1
H.2 Privacy Shield around the PIN Entry Devices .....	H–1
H.2.1 Shielding – Size and Orientation .....	H–1
H.2.2 PIN Entry Device and Numeric Keys .....	H–2
H.3 Shielding – Design Recommendations .....	H–3
H.3.1 Introduction .....	H–3
H.4 Placement and Installation of the terminal .....	H–4
H.4.1 Introduction .....	H–4
H.4.2 Mounting of the PIN Entry Device in the terminal .....	H–4
H.5 Placement of the terminal .....	H–5
H.5.1 Introduction .....	H–5
H.6 Protected access to Card Reader and PIN Entry Device .....	H–6
H.6.1 Access to the inside of the terminal .....	H–6
H.6.2 No operation when the terminal is open .....	H–8
H.6.3 Other Equipment .....	H–8
H.7 Figures .....	H–10
H.7.1 Privacy Shield around the PIN Entry Device .....	H–10

	<b>page</b>
H.7.2 Reference Directions .....	H-11
H.7.3 The Height of the Shielding .....	H-12
H.7.4 Mounting of the PIN Entry Device (Angle) .....	H-13
H.7.5 Height and position of the PIN Entry Device .....	H-14
<b>Attachment I. Gift Voucher / Gavekort .....</b>	<b>I-1</b>
I.1 Flex Terminals and Gavekort .....	I-1
I.1.1 Introduction .....	I-1
I.2 Gavekort Transaction Information .....	I-1
I.3 Accepting Gavekort .....	I-1
I.4 Business Calls for Gavekort Transactions .....	I-1
I.5 How to get the Gavekort Transaction Information? .....	I-2
I.6 Correlation between business and transaction events .....	I-3
I.6.1 Balance inquiry .....	I-5
I.6.2 Loading a Gavekort .....	I-5
I.6.3 Buying with a Gavekort .....	I-5
I.6.4 Buying with a Gavekort When Online Transactions Cannot Be Performed ...	I-6
I.6.5 Loading a Gavekort When Online Transactions Cannot Be Performed .....	I-6
I.7 Dialogue – Merchant and Cardholder .....	I-6
I.8 Error situations .....	I-7
I.9 Receipts .....	I-8
I.9.1 Receipt for a Køb .....	I-8
I.9.2 Receipt for a Køb with Cashback .....	I-9
I.9.3 Receipt for a Saldokontrol .....	I-10
I.9.4 Receipt for a Load .....	I-11
I.9.5 Receipt for an Offline Køb .....	I-12
I.9.6 Receipt for an Offline Load .....	I-13
I.9.7 Receipt in case of no Response for a Køb .....	I-14
I.10 Scanning the bar code on the Gavekort vs. using the magnetic stripe .....	I-14
I.11 Total Reports .....	I-16
<b>Attachment J. Guidelines for Logging .....</b>	<b>J-1</b>
<b>Attachment K. Terms – Business Calls and Administrative Functions .....</b>	<b>K-1</b>
K.1 Introduction .....	K-1
K.2 Business Calls .....	K-1
K.3 Administrative Functions .....	K-2
<b>Attachment L. Defective Advices in Data Store .....</b>	<b>L-1</b>
L.1 Introduction .....	L-1
L.2 Requirements and Principles for the Solution .....	L-1
L.2.1 General .....	L-1
L.2.2 The fifth File (File-5) .....	L-2
L.2.3 Adding records to File-5 .....	L-2
L.2.4 Transfer of records from File-5 .....	L-2
L.2.5 Deleting records from File-5 .....	L-3
L.2.6 Log-information, when a record is deleted from File-5 .....	L-3
L.3 Temporary use while records in File-5 .....	L-4



	page
<b>Attachment M. Guidelines for Usage of the User Interface Display</b> .....	<b>M–1</b>
<b>M.1 Introduction</b> .....	<b>M–1</b>
<b>M.2 Messages for Display based on 16 Characters per Line</b> .....	<b>M–1</b>
<b>M.3 Display flow for Transactions</b> .....	<b>M–6</b>
<b>M.3.1 Example 1: Display flow for PIN Transaction – Approved</b> .....	<b>M–7</b>
<b>M.3.2 Example 2: Display flow for PIN Transaction – PIN Error</b> .....	<b>M–8</b>
<b>M.3.3 Example 3: Display flow for PIN Transaction – PIN Error with PIN retry</b> ....	<b>M–9</b>
<b>M.3.4 Example 4: Display flow for Signature Transaction – Approved</b> .....	<b>M–11</b>
<b>M.3.5 Example 5: Display flow for signature Transaction – Approved</b> .....	<b>M–12</b>
<b>M.4 Display flow for Transactions – max. 16 Characters per Line</b> .....	<b>M–13</b>
<b>M.4.1 Example 1: Display flow for PIN Transaction – Approved</b> .....	<b>M–14</b>
<b>M.4.2 Example 2: Display flow for PIN Transaction – PIN Error</b> .....	<b>M–15</b>
<b>M.4.3 Example 3: Display flow for PIN Transaction – PIN Error with PIN Retry</b> ....	<b>M–16</b>
<b>M.4.4 Example 4: Display flow for Signature – Approved</b> .....	<b>M–18</b>
<b>M.4.5 Example 5: Display flow for Signatue Transaction – Approved</b> .....	<b>M–19</b>
<b>Attachment N. Guidelines for Constructing Total Reports</b> .....	<b>N–1</b>
<b>N.1 Introduction</b> .....	<b>N–1</b>
<b>N.2 General</b> .....	<b>N–1</b>
<b>N.3 Data Elements</b> .....	<b>N–2</b>
<b>N.4 Example</b> .....	<b>N–3</b>
<b>N.5 Proposal for accumulating data for Totalling Reports</b> .....	<b>N–5</b>
<b>N.5.1 Transaction Record – a way to accumulate Totals</b> .....	<b>N–6</b>
<b>N.5.2 Initialization</b> .....	<b>N–7</b>
<b>N.5.3 Data elements filled in during online requests</b> .....	<b>N–8</b>
<b>N.5.4 Data Elements filled in during Transaction Completion</b> .....	<b>N–9</b>
<b>N.5.5 Data elements filled in during transfer of Advices</b> .....	<b>N–9</b>
<b>N.5.6 Result – ‘OK’ or ‘Not OK’</b> .....	<b>N–10</b>
<b>N.5.7 Result – Irrelevant or with no Financial Impact</b> .....	<b>N–11</b>
<b>Attachment O. Merchant Initiative Bypass</b> .....	<b>O–1</b>
<b>O.1 Introduction</b> .....	<b>O–1</b>
<b>O.2 General</b> .....	<b>O–2</b>
<b>O.2.1 General Requirements</b> .....	<b>O–2</b>
<b>Attachment P. Local PIN</b> .....	<b>P–1</b>
<b>P.1 Introduction</b> .....	<b>P–1</b>
<b>P.2 Business Requirements</b> .....	<b>P–1</b>
<b>P.3 Description</b> .....	<b>P–1</b>
<b>P.4 Local PIN Validation Message Flow</b> .....	<b>P–2</b>
<b>P.4.1 Local PIN Validation</b> .....	<b>P–2</b>
<b>P.5 Plaintext PIN Data</b> .....	<b>P–4</b>
<b>P.5.1 Local PIN Validation command – Plaintext PIN</b> .....	<b>P–4</b>
<b>P.6 Enciphered PIN Data</b> .....	<b>P–4</b>
<b>P.6.1 Key Management</b> .....	<b>P–4</b>
<b>P.6.2 Load LP Keys Command</b> .....	<b>P–6</b>
<b>P.6.3 Local PIN Validation command – Enciphered PIN</b> .....	<b>P–7</b>
<b>P.6.4 Get Debit/Credit Properties Command</b> .....	<b>P–10</b>
<b>P.6.5 Complete Payment Command</b> .....	<b>P–10</b>

	<b>page</b>
<b>P.7 Limitations</b> .....	<b>P-10</b>
<b>P.7.1 Enabling/Disabling of the Local PIN Validation functionality</b> .....	<b>P-10</b>
<b>P.7.2 Availability of the Local PIN Validation functionality</b> .....	<b>P-10</b>
<b>P.7.3 PIN Range</b> .....	<b>P-10</b>
<b>P.7.4 PIN tries</b> .....	<b>P-10</b>
<b>P.8 Application Status Words (ASW1-ASW2)</b> .....	<b>P-10</b>
<b>P.9 Message Codes</b> .....	<b>P-11</b>
<b>P.10 Example of Message Flow</b> .....	<b>P-12</b>
<b>Attachment Q. Status of Previous Transactions</b> .....	<b>Q-1</b>
<b>Q.1 Introduction</b> .....	<b>Q-1</b>
<b>Q.1.1 Duplicate Transaction Check performed by the PSAM</b> .....	<b>Q-1</b>
<b>Q.2 Functionality</b> .....	<b>Q-1</b>
<b>Q.2.1 General</b> .....	<b>Q-1</b>
<b>Q.2.2 The Get Debit/Credit Properties Command</b> .....	<b>Q-2</b>
<b>Q.3 Purpose of this Functionality</b> .....	<b>Q-2</b>
<b>Q.3.1 Introduction</b> .....	<b>Q-2</b>
<b>Q.3.2 Reference STAN</b> .....	<b>Q-3</b>
<b>Q.3.3 PAN</b> .....	<b>Q-5</b>
<b>Q.4 Limitations</b> .....	<b>Q-5</b>
<b>Q.4.1 Availability</b> .....	<b>Q-5</b>
<b>Q.4.2 Transaction Types</b> .....	<b>Q-5</b>
<b>Q.4.3 Approved/Successful Transactions</b> .....	<b>Q-5</b>
<b>Q.4.4 Number of Entries</b> .....	<b>Q-6</b>
<b>Q.4.5 PAN</b> .....	<b>Q-6</b>
<b>Attachment R. Implementation Conformance Statement (ICS)</b> .....	<b>R-1</b>
<b>R.1 Introduction</b> .....	<b>R-1</b>
<b>R.2 Implementation Conformance Statement</b> .....	<b>R-1</b>
<b>R.2.1 Configurable Kernel</b> .....	<b>R-1</b>
<b>R.2.2 Legend</b> .....	<b>R-1</b>
<b>Attachment S. Terminals with Combined Cardholder and Merchant Interface</b> .....	<b>S-1</b>
<b>S.1 Introduction</b> .....	<b>S-1</b>
<b>S.2 Conditions and Requirements</b> .....	<b>S-1</b>
<b>S.3 Examples</b> .....	<b>S-3</b>
<b>Attachment Z. Problem Reporting</b> .....	<b>Z-1</b>
<b>Index</b> .....	<b>Index-1</b>

# 1. Revision Log

Version	Date	Last Page	Affects	Brief Description of Change
1.0	2000–01–17		All pages	Initial production release.
2.0A	2000–05–26		See —>	<p>Updated to reflect ref. 39...42 (TAPA).            New document structure for better separation of debit/credit and purse functionality.            Changes based on comments from terminal manufacturers.            Editorial changes.            Amended host messages.</p> <p><b>Released:</b></p> <ul style="list-style-type: none"> <li>Chapter 2: Object and Field of Application</li> <li>Chapter 3: Definitions</li> <li>Chapter 6: Debit/Credit Functionality (selected pages)</li> <li>Chapter 8: Commands and Responses</li> <li>Att. F: Host Communication (debit/credit)</li> </ul>
2.0B	2000–06–xx		See —>	<p>Fewer OTRS–specific terms in chapter 3.            System Overview (chapter 4) released.            New optional command added (Transaction State Information).            Initialization process for debit/credit application released.            Minor technical updates and editorial changes.</p> <p><b>Released:</b></p> <ul style="list-style-type: none"> <li>Prologue: Title page and Disclaimers</li> <li>Chapter 0: Table of Contents</li> <li>Chapter 1: Revision Log</li> <li>Chapter 2: Object and Field of Application</li> <li>Chapter 3: Definitions</li> <li>Chapter 4: System Overview</li> <li>Chapter 6: Debit/Credit Functionality (selected pages)</li> <li>Chapter 8: Commands and Responses</li> <li>Att. A: Magnetic Stripe Formats</li> <li>Att. B: Validation of the PAN</li> <li>Att. C: SDL Notation</li> <li>Att. F: Host Communication (debit/credit)</li> <li>Att. H: Privacy Shielding</li> <li>Att. Z: Problem Report</li> </ul>

2.0C	2000-06-30	Chapter 8	<p>The <i>Installation</i> command has been amended in order to make it possible to convey more terminal information to host. Additional data elements, necessary for printing the receipt, have been added in the response to <i>Initiate EMV Payment</i> command.</p> <p>A <i>Token Based Payment</i> command is added. The ASW1-ASW2 coding is updated accordingly.</p>
2.0C	2000-06-30	Att. F	<p>APACS 60 header now TLV-coded.</p> <p>Field 23 removed from MSC and Key Entered transactions.</p> <p>Field 27 values updated (MTI 0360/0370)</p> <p>Field 37 removed from Authorization messages.</p> <p>Field 56 length corrected.</p>
2.0	2000-07-31	See →	<p>Chapter 7, Purse functions and related attachment(s) released.</p> <p>Minor technical updates and editorial changes.</p> <p><b>Released:</b></p> <ul style="list-style-type: none"> <li>Prologue: Title page and Disclaimers</li> <li>Chapter 0: Table of Contents</li> <li>Chapter 1: Revision Log</li> <li>Chapter 2: Object and Field of Application</li> <li>Chapter 3: Definitions</li> <li>Chapter 4: System Overview</li> <li>Chapter 5: Application-independent Requirements</li> <li>Chapter 6: Debit/Credit Functionality</li> <li>Chapter 7: Purse Functionality</li> <li>Chapter 8: Commands and Responses</li> <li>Chapter 9: Data Elements</li> <li>Chapter 10: Design Requirements</li> <li>Att. A: Magnetic Stripe Formats</li> <li>Att. B: Validation of the PAN</li> <li>Att. C: SDL Notation</li> <li>Att. D: Certification</li> <li>Att. E: Cardholder Activated Terminals</li> <li>Att. F: Host Communication (debit/credit)</li> <li>Att. G: Receipts</li> <li>Att. H: Privacy Shielding</li> <li>Att. I: Multi-drop Interface</li> <li>Att. Z: Problem Report</li> </ul>

2.0	2000–07–31	Chapter 5	Section 5.13.4, Building the H1H2 Selection Table has been added. Previous requirements 5.6.1.11 & 5.6.1.12 are deleted.
2.0	2000–07–31	Chapter 6	<p>In section 6.1.5, a new mechanism for getting the MSC Table data out of the PSAM has been added. Description of the PSAM Shutdown command has been added in section 6.1.8.</p> <p>In table 6.2, the combination “Key Entered”, “Card present” and “No CVM” has been deleted.</p> <p>The Merchant Number has been added to all the Tokens. The sections 6.10 (EMV Transactions), 6.13 (Key Entered Card Transactions), 6.14 (Token Based Transactions) and 6.18 (Exception Handling) have been added. The Advice Window Size mechanism has been slightly modified (section 6.16.1). In section 6.17.3, a subsection “Service Records” has been added which also has an impact on figure 6.27. Furthermore, in section 6.17.3, text has been added to describe handling of Advice Transfer when dealing with several PSAMs supporting Debit/Credit. Two requirements concerning the handling of PSAM Updates have been added in section 6.17.3.</p>
2.0	2000–07–31	Chapter 8	<p>A new requirement concerning “unknown” ASW1–ASW2 values has been added.</p> <p>A new section 8.3 “Error Responses” has been added. A new command, <i>Create Service Record</i>, has been defined. The TAPA defined <i>Synchronize PSAM/PIN Pad</i> command has been added. A new “chaining” mechanism has been added for the <i>Get MSC Table</i> command. A number of new ASWs has been added and the part dealing with PIN errors has been amended.</p>
2.0	2000–07–31	Chapter 9	The data element “CVM Forced” has been renamed to “Merchant Initiative” (MI) in order to reflect that online/offline also can be forced by the merchant. Several data elements have been added.

2.0	2000-07-31	Att. F	In F.2, the section “Primary and Secondary Call Numbers” has extended. In section F.3.1 “Physical Layer”, Requirement are added concerning physical connection. Section F.5 “Transmission Formats” has been amended concerning the APACS header. The sections F.6 (Communication Statistics and Error Counters) and F.7 (Primitive Data Objects for the APACS Header) have been added. Two data elements (error related) have been added in table F.94. Issuer Script Result has been added in table F.97.
2.1	2000-11-30	Chapter 4	The erroneous reference to Attachment E has been updated to Attachment D.
2.1	2000-11-30	Chapter 5	The previous requirement 5.6.5.2 has been deleted as no TAPA command for this purpose is defined. The standard ISO/IEC 8859-9 has been replaced by ISO/IEC 8859-15. Additional requirements concerning the Data Store have been added.
2.1	2000-11-30	Chapter 6	A new requirement is added to section 6.1.7 concerning multiple PIN Pads and synchronization. The column indicating the combination “Key entered”, “Card present” and “No CVM” has been deleted from table 6.2 and 6.7. Track 2 equivalent data has been added to the EMV related Token. New sections 6.6 to 6.8 have been added. The previous requirements 6.13.14.2 to 6.13.14.5 have been removed and inserted in the new sections 6.7.1 and 6.8.2. Section 6.9 has been renamed from “Amount Carrying Transactions” to “Card Related Transactions”. Requirements concerning “Terminal Identification” have been added for the four different card data sources. The selection of the appropriate Card Name has been amended. Concerning the Batch Number, the 6 <i>least</i> significant will be present at the statement of account. In general, a <i>Get KCV</i> command has been added in the transaction figures when the

			<p>PIN Pad is engaged.</p> <p>In section 6.18 “Exception Handling”, requirements concerning PSAM Updates and Advice Transfer have been added.</p>
2.1	2000–11–30	Chapter 8	<p>The two EMV defined commands “Select” and “Read Record” (used for application selection) have been added to table 8.1.</p> <p>The number of Application Status Words considered successful have been extended to contain values in the ‘10XX’ for the <i>Start-up PSAM</i> and <i>Exchange Debit/Credit Static Information</i> commands.</p> <p>CNT<sub>AID</sub> has been changed to support none AIDs.</p> <p>The length for SW1 SW2 (<i>Get Next</i> command) has been amended to 2 bytes.</p> <p>Terminal Identification has been removed from the <i>Install</i> and <i>Exchange Debit/Credit Static Information</i> commands and inserted in the <i>Initiate Payment</i> commands instead.</p> <p>Terminal Type changed from 2 bytes to 1 (according to EMV ’96).</p> <p>Missing parameters for the <i>Add Addendum Record</i> command are added.</p> <p>MAC key has been added to PIN Data in table 8.90.</p> <p>The section describing the ASW1–ASW2 codes has been completely re-designed in order to make it easier for the terminal supplier to determine which action to take. ASW1–ASW2 = ‘17A3’ (Invalid transaction) is changed to ‘1780’ (Invalid transaction).</p>
2.1	2000–11–30	Chapter 9	<p>The format of the Batch Number has been modified.</p>
2.1	2000–11–30	Att. F.	<p>The column ‘C7’ (APACS MAC Key Version) has been deleted in table F.9.</p> <p>Attribute for Key Versions changed from n5 to b1.</p> <p>Attribute for Terminal Approval Number changed from n5 to b2.</p> <p>Field 35 (Track 2 Data) has been added to table F.14, F.20 and F.32 and therefore removed from bit55.</p> <p>Terminal Identification is placed in field 41 (Card accepting device). Terminal</p>

			<p>Identification is not sent in the Install transaction.</p> <p>MAD-Handler ID is placed in field 46 (CAD Management/Service Quality Data).</p> <p>Field 64 (Message authentication code) in the tables F.40 and F.41 has been deleted.</p> <p>Field 30 (Amount, original transaction) has been deleted for all Reversal Advices as partial reversal is not supported by the terminal.</p> <p>Message type 0226 has been added to field 56 in tables F.42, F.46 and F.48.</p> <p>Field 64 (Message authentication code) has been deleted in table F.64.</p> <p>Info Level added to table F.84.</p> <p>Changed attributes for Terminal Type and Terminal Approval Number in table F.84.</p> <p>Tags assigned to all data elements in field 44, 46, 47 and 63.</p> <p>“Signature forced indicator” has been replaced by “Merchant Initiative”.</p>
2.1	2000-11-30	Att. G.	<p>A new requirement (G.1.1.12) has been added.</p> <p>“BUNDT NR:” has been replaced by “PSAM:”. Requirement G.1.2.34 has been updated accordingly.</p> <p>The previous line 36 has been deleted, line numbering has been amended throughout the Attachment.</p> <p>Requirement G.1.2.22 has been amended concerning the format and related data element.</p> <p>Requirements for Reversals have been added.</p>
2.1.1	2001-02-15	Chapter 5	<p>Requirement 5.4.4.11 is deleted.</p> <p>The number of letters in the text fields of table 5.14 (Messages for Display and Printing) has been truncated to 20.</p> <p>The requirements to the contents of the Log has been clarified.</p>
2.1.1	2001-02-15	Chapter 6	<p>Requirements concerning the User Interface Handler have been added.</p> <p>A new definition of the data element ‘Number of PIN Entries Left’ has been introduced.</p> <p>Requirements applicable for the handling of error counters have been added for</p>



			EMV, MSC, Key Entered and Token Based. In general, the MAD–Handler shall first issue the <i>Transaction Completed</i> command after a successful response to the <i>Complete Payment</i> command. The subclause 6.16.9 Clock Synchronization has been enhanced.
2.1.1	2001–02–15	Chapter 8	The commands <i>Exchange Static Debit/Credit Information</i> and <i>Install</i> have been amended due to extension of the Additional Terminal Capabilities field (3 bytes → 5 bytes). A definition of the response to a <i>Validate Data</i> command in case of segment <i>n</i> of <i>m</i> has been added. New ASW codes have been added, especially in the category “Approved/Successful – Action Required”.
2.1.1	2001–02–15	Chapter 10	The requirement concerning landing contacts in the ICCR has been reclassified.
2.1.1	2001–02–15	Att. F	The Tag ‘CF’ (Communication Interface Statistics) has been defined. The length of the APACS header (Tag ‘C0’) is now binary. In the subclause F.9.1, Coding Conventions, the length field are now 2 bytes binary. Valid values for field 21 (POS Capability Code) and 22 (POS Entry Mode) are now defined in table F.84. The values for the data element ‘Download Control’ used in the PSAM Update messages has been clarified. Clarifications has been added.
2.1.2	2001–08–25	Chapter 5	Two new B requirements concerning information field size for the IFD have been added for clarity.
2.1.2	2001–08–25	Chapter 6	Two new figures (6.1 & 6.4) clarifying the initialization– and PSAM/PIN Pad synchronization sequence have been added. Table 6.4 and table 6.7 have been amended according to the allowed CVMs. The data elements contained in the tokens have been adjusted. Table 6.12 has been updated concerning the Refund (only signature is allowed).

			<p>Figure 6.6 in the previous version (EMV Transaction (Refund – PIN) and figure 6.8 (Refund – No CVM) are deleted as refund is only possible using signature.</p> <p>A new clause (6.15) “Addendum Records” has been added.</p> <p>“Disconnect” has been removed from figure 6.27.</p> <p>A new subclause (“Sequence of Events for Advice Transfers”) has been added.</p> <p>The coding of the Message Number in Download Control (field 27) for PSAM Updates has been clarified.</p>
2.1.2	2001-08-25	Chapter 8	<p>The definition of the MAD-Handler ID has been amended.</p> <p>The data element ME<sub>BRN</sub> (Merchant Business Registration Number) has added in the response to <i>Exchange Debit/Credit Static Information</i> command.</p> <p>The Add Addendum Record command has been adjusted according to the functionality described in clause 6.15.</p> <p>The definition of the field “Transaction Status” in the Complete command has been clarified.</p> <p>The length field LEN<sub>TOKEN</sub> in the <i>Complete Payment</i> commands and LEN<sub>DATA</sub> in <i>Get Merchant Data</i> command has been extended to two bytes.</p> <p>The data element “MI” (Merchant Initiative) and data elements concerning amounts have been added to the <i>Initiate Token Based Payment</i> command.</p> <p>A new table (8.107) giving the Message Codes for ranges of ASW1-ASW2 has been added.</p> <p>New ASW1-ASW2 codes have been added, especially in the category “Approved/Successful – Action Required”.</p>
2.1.2	2001-08-25	Chapter 9	<p>The data elements Approval Code, Type of Application, ME<sub>BRN</sub> and Mad-Handler ID, Terminal Manufacturer ID and Terminal Serial Number have either been amended or added.</p> <p>The coding of Merchant Initiative (MI) has been extended to cover attaching of addendum records as well.</p>
2.1.2	2001-08-25	Att. F	<p>Clarifications has been added.</p> <p>A Financial Request concerning ICC (Re-</p>

			fund) has been added. Field 64 (message authentication code) have been removed from the following tables: F.21, F.23, F.25, F.33, F.35, F.37, F.39, F.43, F.47, F.49, F.51 and F.53. This field is never verified by PSAM nor by the terminal. New tables regarding POS Entry Mode have been added for clarification. The format of “Card reconciliation Counter ID” has been changed from n3 to an3.
2.1.2	2001–08–25	Att. G	A new note describing the conditions for for printing the Application Effective Date has been introduced. Clarifications have been added.
2.1.2	2001–08–25	Att. J	This Attachment has been added.
2.1.2	2001–08–25	Att. K	This Attachment has been added.
2.1.2	2001–08–25	Att. L	This Attachment has been added.
2.2	2002–07–05	All pages	The reference to the EMV specifications has been changed from “EMV’96: 1998 Version 3.1.1” to “EMV 2000: Version 4.0, December 2000”.
2.2	2002–07–05	Chapter 3	The reference number 58 ‘Terminal Requirements for Acceptance of Chip Pay Now (Debit) and Pay Later (Credit) Cards’ has been moved from section 3.5 Bibliography to section 3.4 References. The reference number 59 ‘Visa Integrated Circuit Card. Terminal Specification’ has been moved from section 3.5 Bibliography to section 3.4 References. The references 23, 24, 25 “EBS 105” have been moved from section 3.5 Bibliography to section 3.4 References.
2.2	2002–07–05	Chapter 4	Section 4.8.2 has been updated to clarify the certification process. The PED approval process is now explicitly included.
2.2	2002–07–05	Chapter 5	A new section has been introduced for clarification purposes. The new section is called ‘Fallback from Chip (ICC) to Magnetic Stripe (MSC)’ and this section defines the requirements

<p>for fallback from chip technology to magnetic stripe technology.  A new section 5.15 (Language Selection) has been introduced.  Additional information has been added to section 5.2 concerning protected functions.  The data element Application Selection Indicator has been introduced in section 5.13.5.  Two new requirements concerning cardholder confirmation during application selection have been added.  In section 5.6.1, the PED evaluation procedures to follow is added as a reference to Attachment D.</p>	<p>2.2      2002-07-05              Chapter 6</p>	<p>Figure 6.1 has been amended.  Requirements 6.1.2.4 and 6.16.3.9 have been modified for clarification.  Two new requirements are inserted at the end of the section “Retrieval of the Token”.  Requirement 6.16.5.1 is modified and a new requirement has been added.  A note shall be added to requirement 6.15.1.7.  The requirement 6.18.6.1 has been shortened and two notes have been added for clarification.  A new requirement 6.2.6.1 has been added concerning cashback.  The requirement 6.18.4.4 has been updated to prevent misunderstanding.  A new figure 6.31 has been added.  The requirements 6.14.4.1 and 6.14.4.2 have been updated, and a new requirements have been added 6.1.4.4.3.  Additional text and requirements concerning the handling of Cardholder initiated exceptions will be added for clarification purposes.  New text is added to section 6.16.11.  Additional text concerning the handling of Merchant initiated exceptions will be added for clarification purposes.  A new section 6.16.17 will be added.  A new section 6.18.18 is added.  The text and the note stated below table 6.17 has been amended.  Section 6.10.4 has been amended con-</p>
---	---	--

			<p>cerning the <i>Check Stop List</i> command. This includes amendments in the figures 6.7, 6.8, 6.9 and 6.10.</p> <p>The requirements 6.10.3.10 – 6.10.3.11 is updated concerning FCI.</p> <p>Introduction of a new header (concerning tokens) has been added in tables 6.8, 6.9, 6.10 and requirements have been added in section 6.14.2.</p>
2.2	2002–07–05	Chapter 8	<p>Last row in table 8.76 has been deleted.</p> <p>In table 8.107, the last range ('17B0' – 'FFFF') has been split up into four different ranges Last row in table 8.118 has been deleted.</p> <p>The data element ATC returned in the response to <i>Initiate EMV Payment</i> command has been moved to response of <i>EMV Payment</i> command.</p> <p>The data element ATC has been deleted from the response to <i>Initiate Token Based Payment</i> and added in the command <i>Token Based Payment</i>.</p> <p>The Message Codes defined in table 8.107 have been amended.</p> <p>Requirement 8.8.1.4 has been added.</p> <p>The data element "PAN<sub>SEQUENCE</sub>" shall be included in the response to <i>Initiate Token Based Payment</i> in table 8.67.</p> <p>New ASWs have been added to table 8.109 to 8.121.</p> <p>The format of the <i>Initiate EMV Payment</i> command is modified, see table 8.38.</p> <p>Requirements 8.6.4.2 &amp; 8.6.4.3 have been corrected.</p> <p>Note under table 8.44 has been corrected as well.</p> <p>A new requirement 8.6.20.2 has been added.</p>
2.2	2002–07–05	Chapter 9	<p>The data element list in section 9.2.62, the format is corrected from 'n6' to 'an6'.</p> <p>The maximum size of the data element Statistics is 42 bytes, and not 48 as stated previously.</p>
2.2	2002–07–05	Att. B	<p>A note shall be added to requirement B.1.1.1 concerning the Luhn formula.</p>
2.2	2002–07–05	Att. D	<p>The Attachment has been updated to reflect the development and certification of a terminal, only.</p>

			<p>Requirements to the PED evaluation process have been added as well as references to standards for the security evaluation. A number of EMVCo related requirements have been added or reflected in the original text.</p>
2.2	2002-07-05	Att. F	<p>A new requirement shall be inserted at the end of the section F.3.6.</p> <p>The example stated section F.9.1 shall be corrected.</p> <p>Adjustments of the messages have been done.</p> <p>The row for field 46 – “Cad management/service quality data” has been updated.</p> <p>A new table F.95 has been added to section ‘F.9.11 TLV Coding of Field 46’.</p> <p>In field 55 a new data element Transaction Status Information (TSI) has been added for audit purposes.</p>
2.2	2002-07-05	Att. G	<p>In table G.5 the description for Authorization has been changed and two rows have been added.</p> <p>Line 14 of the receipt shall include both Card Name and PAN Sequence Number.</p> <p>A new requirements G.1.2.19 has been added.</p> <p>Table G.5 “Transaction Condition Codes” is updated to indicate that PIN and Signature may be combined as CVM.</p>
2.2	2002-07-05	Att. J	<p>Page J-6 to J-8 has been updated according to requirements in section 6.</p>
2.2	2002-07-05	Att. N	<p>A new attachment N called “Guidelines for Usage of the User Interface Display” has been introduced.</p>
2.2	2002-07-05	Att. O	<p>A new attachment O called “Guidelines for Constructing Total Reports” has been introduced.</p>
2.2.1	2003-04-02	Chapter 3	<p>The ISO 9564-1:2002 has been updated.</p>
2.2.1	2003-04-02	Chapter 4	<p>The chapter has been revised and changed editorially.</p> <p>The introduction to certification has been augmented.</p>
2.2.1	2003-04-02	Chapter 5	<p>Requirement 5.6.4.22 has been added to be more specific concerning displaying of</p>

			<p>Currency Code.</p> <p>The previous section 5.5.6 (Sub–handler, ICCR – Memory Card Reader) has been deleted as it is considered obsolete.</p> <p>Requirements concerning the interface to the PSAM have been added to be more precise.</p> <p>A new section 5.13.6 (Combined MSC and ICC Application Selection) is added in order to handle terminals equipped with a combined reader.</p> <p>The data element ASI has been introduced.</p> <p>Section 5.14 (Fallback) has been extended extensively to incorporate requirements from all major card schemes available.</p>
2.2.1	2003–04–02	Chapter 6	<p>Figure 6.2 &amp; 6.1 have been amended in order to incorporate handling of ASI and correct an ASW1–ASW2 error.</p> <p>Requirements concerning Advice Transfer and Advice Window Size have been added to be more precise.</p> <p>Table 6.31 has been amended.</p> <p>A new section 6.18.6 “Host Declined Transactions (Requests)” has been added to describe the PIN retry handling in more details.</p> <p>Requirement 6.18.16.1, previously an A requirement is now a C requirement.</p>
2.2.1	2003–04–02	Chapter 7	<p>References to Memory Cards/Disposable Cards (and related subjects) have been deleted.</p>
2.2.1	2003–04–02	Chapter 8	<p>A new command <i>Get Debit/Credit Properties</i> has been introduced to retrieve additional data from the PSAM.</p> <p>A new ASW1–ASW2 = ‘10FF’ (Incorrect PIN, next CVM selected) is added for indicating incorrect PIN when offline PIN is validated.</p> <p>Message Codes Vs. ASW1–ASW2 ranges has been amended.</p> <p>Purse commands related to memory cards have been deleted as they are not to be supported in the future.</p>
2.2.1	2003–04–02	Chapter 9	<p>“ASI”, “Card Service Info” and “Service Code” have been added to the list of data elements.</p>

2.2.1	2003-04-02	Chapter 10	A new section 10.4.3 (Additional Requirements to the PED Software) has been added.
2.2.1	2003-04-02	Att. D	Substantial changes to address the complexity of the EMV related certification processes. As most of this Attachment is rewritten, no revision bars are present.
2.2.1	2003-04-02	Att. F	Field 39 (Action Code) has been added in inbound messages. Clarifications has been introduces. Authorization Response Code has been added in field 55.
2.2.1	2003-04-02	Att. G	A new subsection “Guidelines for failed or rejected ICC Transactions” has been introduced for clarification. Section G.2 “Receipt Variants” is added. It is now recommended that ASW1-ASW2 are printed on the receipt. Additional information are added concerning Reversals due to technical problems. Table G.4 has been extended to cover PAN length from 7 digits and upwards. A note has been added to table G.5 for clarification.
2.2.1	2003-04-02	Att. O	A new section N.5 “A proposal for accumulating data for Total Reports” has been introduced.
2.3	2003-10-13	Chapter 3	Voice authorization has been added to the list of “Terms”.
2.3	2003-10-13	Chapter 5	A new requirement 5.1.1.2 concerning ICC & magnetic stripe cards has been added. Requirement 6.7.1.13 concerning Business Calls and display messages has been added. In figure 5.1, text referred to at the Cardholder Display has been amended to be in line with the Message Codes already defined.
2.3	2003-10-13	Chapter 6	Table 6.3 has been amended in order to reflect the last changes concerning Tokens. A new requirement 6.4.2.7 concerning signature verification has been added. In section 6.5.1, new requirements regard-



			<p>ing Tokens have been added.</p> <p>In section 6.7.1, table 6.11 (Business Calls Vs. Message Codes) is added and several requirements have been added for clarification.</p> <p>In section 6.8.2, an requirements 6.8.2.2 concerning Action Codes has been added. Clarifications concerning error counters &amp; Approval Codes have been added for EMV, MSC, Key Entered and Token based transactions.</p> <p>Clarification regarding Advice Windows has been added in section 6.16.1.</p> <p>A note explaining the relationship between PSAM clean-up and the release of the thread has been added in section 6.18.2.</p>
2.3	2003–10–13	Chapter 8	<p>The commands described in section 8.6.14 and 8.6.16 have been amended.</p> <p>Stop List Status has been amended several places.</p> <p>New ASW1–ASW2s have been added.</p>
2.3	2003–10–13	Chapter 9	<p>MTI, MTI of the Original Message, Reference STAN have been added.</p>
2.3	2003–10–13	Chapter 10	<p>Requirements concerning Audio feedback in section 10.2.8 have been added for clarification.</p>
2.3	2003–10–13	Att. F	<p>The tags ‘D1’ and ‘D2’ have been introduced.</p> <p>In addition the tags TE, TF, TG and TH related to error counters have been added.</p> <p>In figure F.13, the row “Bearer Network” has been extended with new options.</p>
2.3	2003–10–13	Att. G	<p>New requirements concerning line 35 of the receipt have been added.</p>
2.3	2003–10–13	Att. O	<p>The impact on the reports when introducing ‘D1’ and ‘D2’ have been added.</p>
2.3	2003–10–13	Att. P	<p>A new Attachment P (Merchant Initiative Bypass) has been added. It describes the possibilities for the merchant to alter the CVM or the requirements for online/off-line transactions.</p>
2.4	2004–03–01	Chapter 3	<p>A reference to “TAPA version 2.1, February 2001, <i>Application Architecture Specification – Errata</i>” has been added.</p>

2.4	2004-03-01	Chapter 5	<p>A new requirement 5.13.5.2 concerning the minimum number of entries in the Candidate List has been added.</p> <p>The definition of a combined reader has been extended.</p> <p>Fallback handling for combined readers (ICC before MSC) is added.</p>
2.4	2004-03-01	Chapter 6	<p>A new subsection 6.3, “Gratuity and other surcharges” has been added for clarification.</p> <p>The definition of <math>LEN_{A+B}</math> is corrected in table 6.10.</p> <p>Subsection 6.7.1 has been extended for clarification.</p> <p>In section 6.10.4, 6.12.4 and 6.13.4, the handling of Stop List has been extended and figure 6.5 added.</p>
2.4	2004-03-01	Chapter 8	<p>New commands contained in Service Pack No. 1 (<i>Get Debit/Credit Properties &amp; Validate Data 2</i>) are added.</p> <p>New ASW1-ASW2 value are added in order to enhance the fault diagnostics.</p>
2.4	2004-03-01	Chapter 9	<p>The following data elements have been introduced: ID<sub>PSAM</sub>, ID<sub>PSAMCREATOR</sub>, PSAM D/C Life Cycle State, PSAM Subversion, PSAM Version, Service Packs Supported.</p> <p>CVM Status indicates now whether the transaction has been performed as fallback or not.</p> <p>Info Level indicates now whether Confirm Amount is requested or not during Original Authorization.</p>
2.4	2004-03-01	Chapter 11	<p>A new section 11 “Service Packs” is added.</p>
2.4	2004-03-01	Att. F	<p>In table F.1 a new layer (HDLC/X.75) is added.</p>
2.4	2004-03-01	Att. G	<p>The ATC (Application Transaction Counter) is now defined as decimal digits.</p> <p>The impact on receipts due to the introduction of the <i>Validate Date 2</i> command have been added.</p> <p>Handling of ASW1-ASW2 on the receipt is added.</p> <p>A new subsection G.2.6 “Reversal (Authorization)”, G.2.11 “Cashback, Addi-</p>

---

			tional Fees etc.” and G.5 “Receipts printed, depending on Business Environment and actual CVM” are added. In table G.4, the truncation has been extended so only the last 4 digits of the card number are visible.
2.4	2004–03–01	Att. M	A new section L.3, “Temporary use while records in File–5” is added.
2.4	2004–03–01	Att. N	Notes concerning number of PIN tries left are added.
2.4	2004–03–01	Att. Q	A new Attachment P “Local PIN” has been added. Text and requirements to be defined.
2.5	2006–03–01	General	The latest version of the OTRS can be found on the following address: <a href="http://www.pbs.dk/certificering">http://www.pbs.dk/certificering</a> The related Errata can be found here as well.

This page is intentionally left blank

## 2. Object and Field of Application

### 2.1 Target Group

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

### 2.2 Objectives

The purpose of this specification is to enable the manufacturers to develop their products in such a way that any debit or credit and/or purse card based on magnetic stripe technology and/or 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 the manufacturers to develop their products in such a way that all types of cards for which PBS is the acquirer, can be used.

It is aimed that cards, where PBS is not the acquirer, can be supported by the terminal as long as the specified security level is maintained.

Terminals can be used for payments, cash advance or other services according to the functional requirements and recommendations specified by PBS.

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 PBS. The cardholder may in some situations sign a receipt, i.e. use signature as Cardholder Verification Method (CVM) instead of PIN.

The objective is also to ensure that cardholders encounter similar user interfaces, procedures and documentation, e.g. display texts, PIN entry and receipts, when performing payment transactions in different terminals.

### 2.3 Scope

The scope of the specification is the areas where PBS as a card organisation are responsible, i.e. the national and international

regulations including the overall security in terminals for the future.

Terminals are a relationship between the terminal supplier and the merchant with the consequence that if the merchant desires enhanced possibilities in the terminal, e.g. a loyalty scheme, then the merchant must enter agreement about this with the terminal supplier. This specification does not prevent such possibilities as the terminal architecture has been chosen to be open for other terminal applications.

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. 39...42).

The terminal may accept debit/credit cards, purse cards or both. Accepting debit/credit cards always implies reading of magnetic stripe cards as well as IC Cards.

## 2.4 Level of Detail

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” thereby 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”.

The specification is based on a number of documents, e.g. industry specifications like EMV and TAPA and international

standards from ISO and CEN. In order not to have redundant information, this specification does not, as a general rule, copy information in referenced documents.

PBS 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 and the last attachment (Z) is a problem report which may be used when reporting missing issues, errors, inconsistencies or uncertainties.

## 2.5 Document Structure

This specification is organized in the following chapters:

Chapter **0** provides the table of contents, including figure and table lists.

Chapter **1** is the revision log giving the history of the document up to the version in hand.

Chapter **2** (this one) defines the objective and scope for this document and explains the structure of the entire specification.

Chapter **3** states interpretation of abbreviations and specific terms as well as a survey of standards and documents referred to in this specification.

Chapter **4** is the system overview giving an overall description of the terminal, the business requirements and their related high level functional requirements.

Chapter **5** defines the general functional requirements to the terminal, irrespective of the application(s) implemented.

Chapter **6** defines the functional requirements specific to the debit/credit application.

Chapter **7** defines best practice for terminal suppliers & integrators.

Chapter **8** defines the exact formats for commands and responses in the terminal.

Chapter **9** defines the detailed formats of data elements conveyed in commands and responses in the terminal.

Chapter **10** states all requirements for the design of the terminal.

Chapter **11** defines the definition of Service Packs and requirements concerning Service Packs.

Attachment **A** defines magnetic stripe card formats.

Attachment **B** specifies the verification of the primary account number (PAN) using Luhn formula.

Attachment **C** introduces the SDL notation used throughout this specification.

Attachment **D** describes the certification procedures.

Attachment **E** describes the Cardholder Activated Terminals (CATs).

Attachment **F** describes the interface and communication to PBS. Also, the message formats are defined here.

Attachment **G** specifies the receipts for the cardholder and the merchant.

Attachment **H** describes the requirements to the PIN privacy shield.

Attachment **I** gives guidelines for the handling of gift vouchers based on magnetic stripe cards.

Attachment **J** is void.

Attachment **K** provides a translation of the Business Calls and Administrative Functions from English into Danish terms.

Attachment **L** provides means to handle defective Advices in the Data Store.

Attachment **M** gives guidelines for using the User Interface.

Attachment **N** gives guidelines or examples concerning how to design the Total Reports.

Attachment **O** gives guidelines or examples concerning how to design and implement Merchant Initiative Bypass.

Attachment **P** will describes the possible handling of a Local PIN.

Attachment **Q** describes how the terminal can obtain status of the previous transaction from the PSAM.

Attachment **R** gives guidelines for how to fill in the EMVCo Implementation Conformance Statement (ICS).

Attachment **S** describes additional requirements for terminals with combined Cardholder and merchant interface.

Attachment **Z** contains a problem report. Please, do not hesitate to use it in case of omissions, inconsistencies or uncertainties.



## 3. Definitions

### 3.1 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.

### 3.2 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 that are used in their traditional meaning within the payment industry are not defined here 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 8 and data elements are defined in chapter 9.

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

#### 3.2.1 Abbreviations

<b>AID</b>	: Application Identifier
<b>AAC</b>	: Application Authentication Cryptogram, EMV
<b>AAR</b>	: Application Authorization Referral, EMV
<b>APE</b>	: Accelerated PIN Entry
<b>ARQC</b>	: Authorization Request Cryptogram, EMV
<b>ASN.1</b>	: Abstract Syntax Notation, One
<b>ASW</b>	: Application Status Word
<b>ATR</b>	: Answer-to-Reset
<b>CA</b>	: Certificate Authority
<b>CAD</b>	: Card Accepting Device
<b>CAM</b>	: Card Authentication Method, EMV
<b>CAT</b>	: Cardholder Activated Terminal
<b>CDA</b>	: Combined DDA/Application Cryptogram Generation, EMV
<b>CEP</b>	: Common Electronic Purse

<b>CLA</b>	: CLAss byte
<b>CRC</b>	: Cyclic Redundancy Check
<b>CVM</b>	: Cardholder Verification Method, EMV
<b>CVR</b>	: Cardholder Verification Rule, EMV
<b>DAPE</b>	: Dankort Accelerated PIN Entry
<b>DDA</b>	: Dynamic Data Authentication, EMV
<b>(D)EBS</b>	: (Draft) European Banking Standard, ECBS
<b>DS</b>	: Data Store
<b>ECBS</b>	: European Committee for Banking Standards
<b>ECR</b>	: Electronic Cash Register
<b>EFT-POS</b>	: Electronic Funds Transfer at Point of Service
<b>EMV</b>	: Europay, MasterCard and Visa
<b>IC</b>	: Integrated Circuit
<b>ICC</b>	: Integrated Circuit Card (chip card)
<b>ICCR</b>	: Integrated Circuit Card Reader
<b>ICS</b>	: Implementation Conformance Statement
<b>IFD</b>	: Interface Device
<b>INS</b>	: INSTRUCTION code
<b>ISO/IEC</b>	: International Organization for Standardization/ International Electrotechnical Commission
<b>KEK</b>	: Key exchange key
<b>KCV</b>	: Key Check Value
<b>LRC</b>	: Longitudinal Redundancy Check
<b>MAC</b>	: Message Authentication Code
<b>MAD</b>	: Multi-Application Driver (TAPA)
<b>MCC</b>	: Merchant Category Code
<b>MSC</b>	: Magnetic Stripe Card
<b>MSCR</b>	: Magnetic Stripe Card Reader
<b>PAN</b>	: Primary Account Number
<b>PBS</b>	: PBS A/S
<b>PED</b>	: PIN Entry Device (PIN pad)
<b>PK</b>	: Public Key
<b>PIN</b>	: Personal Identification Number
<b>POS</b>	: Point of Service
<b>PPK</b>	: PIN Protection Key
<b>PPS</b>	: Protocol and Parameters Selection
<b>PSAM</b>	: Purchase Secure Application Module
<b>RFU</b>	: Reserved for Future Use
<b>RID</b>	: Registered Application Provider Identifier
<b>PP</b>	: PIN Pad
<b>SAM</b>	: Secure Application Module
<b>SDA</b>	: Static Data Authentication
<b>SK</b>	: Secret Key (DES) or Private Key (RSA)
<b>T.B.D.</b>	: To Be Defined
<b>TC</b>	: Transaction Certificate
<b>VPKI</b>	: Public Key Index

Abbreviations not mentioned here are Data Elements, see chapter 9.

### 3.2.2 Terms

<b>Authorization,</b>	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 laid out by the card issuer.
<b>Business Call,</b>	transaction related information sent from the Merchant Application to the MAD–Handler.
<b>Cardholder Display,</b>	the display for use by the cardholder.
<b>Communication Session,</b>	the communications steps from the terminal initiates a connection, until this session is either closed intentionally or interrupted unintentionally.
<b>Dankort,</b>	the national debit card issued by participants in PBS. 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.
<b>Multi–entry,</b>	functionality in the PSAM which allows several transactions (threads) to be processed “simultaneously”.
<b>PBS PSAM,</b>	the PSAM containing the PBS 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.
<b>Point of Service,</b>	the merchant location from where the card transaction originates.
<b>Single Unit Terminal,</b>	an attended terminal designed to be operated by both the merchant and the cardholder using the same display and keyboard.
<b>Terminal Operator,</b>	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.
<b>Terminal Supplier,</b>	the entity developing manufacturing terminals and supply them to the merchants.
<b>Test House,</b>	the entity performing certification of the terminal.
<b>Token,</b>	a string of bytes created by a PSAM as a result of an Authorization transac-

<b>Transaction,</b>	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.
<b>Visa/Dankort,</b>	a debit Card which, in Denmark, is always used as a Dankort debit card and which abroad is used as a Visa debit card with special restrictions.
<b>Voice Authorization,</b>	is the procedure used by the merchant to obtain approval for an offline transaction (phone call to the Acquirer's helpdesk) .

### 3.2.3 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:

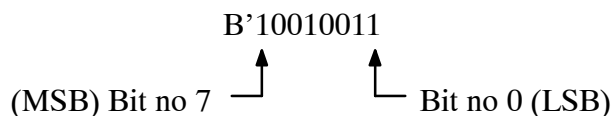


Figure 3.1 – Bit Numbering

#### 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).  
`B1 || B2` Concatenation of bytes B<sub>1</sub> (the most significant byte) and B<sub>2</sub> (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 because every 8th bit of the 64-bit key takes on the value of a parity bit, thereby ensuring that there are 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 Attachment F:

a = alphabetic characters, see ref. 15: “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. 3: “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.

### 3.3 Requirement Numbering

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

**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) PBS 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.

## 3.4 References

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

1. ISO 4217:2001  
*Codes for the representation of currencies and funds.*
2. ISO/IEC 7810:2003  
*Identification Cards – Physical characteristics.*
3. ISO/IEC 7811–2:2001  
*Identification cards – Recording technique – Part 2: Magnetic stripe.*
4. ISO/IEC 7812–1:2000  
*Identification cards – Identification of issuers – Part 1: Numbering system.*
5. ISO/IEC 7813:2001  
*Identification cards – Financial transaction cards.*
6. ISO/IEC 7816–1:1998  
*Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics.*
7. ISO/IEC 7816–2:1999  
*Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.*
8. ISO/IEC 7816–3:1997  
*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/IEC 7816–10:1999  
*Identification cards – Integrated circuit(s) cards with contacts – Part 10: Electronic signals and answer to reset for synchronous cards.*
11. ISO 8583:1987  
*Financial transaction card originated messages – Interchange message specifications.*
12. ISO 8583:1993  
*Financial transaction card originated messages – Interchange message specifications.*
13. ISO/IEC 8825–1:2002  
*Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

14. ISO/IEC 8877-1:1992  
*Information technology — Telecommunications and information exchange between systems — Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T*
15. ISO/IEC 8859-15:1999  
*Information technology – 8-bit single-byte coded graphic character sets – Part 15: Latin alphabet No. 9*
16. ISO 9564-1:2002  
*Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques.*
17. ISO 9564-2:2005  
*Banking – Personal Identification Number management and security – Part 2: Approved algorithm(s) for PIN encipherment.*
18. ISO 11568-2:1994  
*Banking – Key management (retail) – Part 2: Key management techniques for symmetric ciphers.*
19. ISO 11568-3:2005  
*Banking – Key management (retail) – Part 3: Key life cycle for symmetric ciphers.*
20. ISO 11568-4:1998  
*Banking – Key management (retail) – Part 4: Key management techniques using public key cryptosystems.*
21. ISO 11568-5:1998  
*Banking – Key management (retail) – Part 5: Key life cycle for public key cryptosystems.*
22. ISO 13491-1:1998  
*Banking – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods.*
23. ISO 13491-2:2000  
*Banking – Secure cryptographic devices (retail) – Part 2: Security compliance checklists for devices used in magnetic stripe card systems.*
24. MasterCard International  
*Payment Card Industry Data Security Standard, January 2005.*
25. Payment Card Industry (PCI):  
*POS PIN Entry Device Security Requirements Manual  
VERSION 1.3  
February 2005*
26. EN 726-4:1994  
*Identification card systems – Telecommunications integrated circuit(s) cards and terminals – Part 4: Application independent card related terminal requirements.*



27. ENV 1375–1:1994  
*Identification card systems – Intersector integrated circuit(s) card additional formats – Part 1: ID–000 card size and physical characteristics.*
28. EN 41 003, Issue 1, 1991–05–15  
*Particular safety requirements for equipment to be connected to the telecommunications network.*
29. EN 50 (EEC EMC Directive, edited by CLC/TC110)  
*EN 50 081: Generic Emission Standard*  
*EN 50 082: Generic Immunity Standard*
30. EN 55 022  
*Limits and methods of measurement of radio interference characteristics of information technology equipment.*
31. EN 60 529  
*Degrees of protection provided by enclosure IP CODE.*
32. EN 60 950, Issue 1: 1988–06–21  
*Safety of information technology equipment including electrical business equipment.*
33. FIPS Publ. 180–1, 1995–04–17  
*Secure Hash Standard.*
34. CCITT V.24: 1988  
*List of interchange circuits between data terminal equipment (DTE) and data circuit–terminating equipment (DCE).*  
CCITT volume VIII Fascicle VIII.1.
35. CCITT Z.100: 1988,  
*CCITT Specification and Description Language, SDL.*
36. EMV: May 2004, Version 4.1  
*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](http://www.emvco.com).
37. EMVCo Type Approval,  
*Terminal Level 2, Test Cases, Version 4.1.a*  
*February 1st, 2006*
38. APACS Standard 60: 2000–01–01, Version 3  
*UK Specification for message interchange between Card Acceptor & Acquirer.*
39. Terminal Architecture for PSAM Applications (TAPA),  
version 2.0, April 2000  
*Overview*

40. Terminal Architecture for PSAM Applications (TAPA),  
version 2.1, February 2001  
*Application Architecture Specification*
41. Terminal Architecture for PSAM Applications (TAPA),  
version 2.1, February 2001  
*Application Architecture Specification*  
*Errata version 1.1 2004-03-12*
42. Terminal Architecture for PSAM Applications (TAPA),  
version 2.1, February 2001, volume 1  
*Common Electronic Purse (CEP) PSAM Application*
43. Visa Integrated Circuit Card. Terminal Specification,  
Version 1.4.0, Effective 31 October 2001, Amended Sep-  
tember 2005  
published by:  
Visa International
44. M/Chip Functional Architecture – For Debit and Credit  
January 2006  
published by:  
MasterCard International Incorporated.
45. JCB Terminal Specification  
Version 1.2, April 2001  
published by:  
JCB Co., Ltd
46. Amendments to “JCB Terminal Specification  
Version 1.2, April 2001”  
2002-02-12  
published by:  
JCB Co., Ltd
47. AEIPS Terminal Specification,  
(AEIPS 4.1), February 2005  
published by:  
American Express
48. Technical Reference Guide – OTRS Test Specification  
Version 2.0, 2003-05-12  
published by:  
PBS A/S
49. Dankort-håndbogen, published by:  
Dankort A/S  
Lautrupbjerg 10, Postboks 81  
2750 Ballerup
50. Publication 11/89 (Circular no. 27) published by:  
Telestyrelsen  
Islands Brygge 81  
DK-2300 Copenhagen S  
Tel. +45 31 54 47 96  
Fax +45 31 54 48 30.

## 3.5 Bibliography

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

51. ISO 639–1:2002  
*Codes for the representation of names of languages – Part 1: Alpha–2 code.*
52. ISO/IEC 7816–4:1995  
*Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange.*
53. ISO 10202–6:1994  
*Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 6: Cardholder verification*
54. ISO 11568–1:2005  
*Banking – Key management (retail) – Part 1: Introduction to key management.*
55. ISO 11568–6:1998  
*Banking – Key management (retail) – Part 6: Key management schemes.*
56. CR 1750:1999  
*Identification card systems – Inter–sector messages between devices and hosts – Acceptor to acquirer messages.*  
(CEN/TC224)
57. ECBS DEBS 100, March 2004  
*Keyboard layout for ATM and POS PIN Entry devices.*

## 3.6 Related Websites

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

- [www.pbs.dk](http://www.pbs.dk)
- [www.dankort.dk](http://www.dankort.dk)
- [www.mastercard.com](http://www.mastercard.com)
- [www.visa.com](http://www.visa.com)
- [www.emvco.com](http://www.emvco.com)
- [www.ecbs.org](http://www.ecbs.org)
- [www.ecbs.com](http://www.ecbs.com)
- [www.jcbinternational.com](http://www.jcbinternational.com)

This page is intentionally left blank

## 4. System Overview

### 4.1 Introduction

This chapter provides the basic overview and prerequisites for reading and understanding the remaining part of this specification. It includes the historical background as well as new business requirements ending up as technical requirements in the subsequent chapters.

#### **Rationale for this new Terminal Specification**

PBS being both an acquirer and a Terminal Operator in the Danish market sees an opportunity in setting up an open terminal environment taking the new chip card technology into account as a natural development in the terminal industry.

Moreover, this is a consequence of the fact that PBS is the acquirer in Denmark for international Eurocard, JCB, MasterCard and Visa transactions, and thereby must oblige with the rules set by these card schemes, including the rules for migration to chip cards.

This Open Terminal Requirement Specification (OTRS) is developed by PBS on behalf of the Danish banking industry in which banks may act as acquirers and issuers themselves.

This specification contains all requirements to fulfil when building a terminal with a given profile, e.g. a stand-alone POS terminal for debit/credit cards, or a vending machine for debit/credit cards.

As the chip card will be one of the future important technology changes for debit and credit cards, the OTRS terminal must be able to handle such cards according to the EMV specifications issued by the international card schemes: Europay, MasterCard and Visa.

EMV and the introduction of the specifications for a common electronic purse (CEP) have created the foundation for a new terminal giving both merchants and cardholders new means of payment.

## 4.2 Background

### 4.2.1 History

#### **PIN-based Terminals**

The first EFT-POS terminals in the Danish market were introduced in 1984 as stand-alone PIN-based terminals for the Danish debit card system, “Dankort”. At this time, chip cards were not commercially available and standards for chip cards were even less existing.

The PIN-based terminal still only exists in a few proprietary models for the Danish market from a single manufacturer, and was initially delivered according to an agreement with the Danish tele communication operators. Since the original agreements, the Danish telecommunication market has been opened to allow more operators to exist in the market.

The first terminals build to this specification appeared in 2001 for magnetic stripe use only. In 2003 the first EMV compliant terminals was approved by EMVCo.

#### **Signature-based Terminals**

A signature-based terminal was introduced in 1991 and various models from various manufacturers have since been delivered. These terminals generally obtain card authorization by an on-line transaction and deliver batches for clearing and settlement at the end of the day.

### 4.2.2 Standards

The current terminals are only capable of handling magnetic stripe cards where the emerging chip card technology sets up new demands on the terminal infrastructure consisting of terminals and communications network as well as acquirer and issuer host systems.

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 magnetic stripe cards and for chip cards as well as for cryptography and data communication.

### **EMV (Debit/Credit Applications)**

The international card schemes are pushing 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 Europay, MasterCard and Visa.

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

**NOTE:** Maintenance of the EMV specifications has been given to EMVCo ([www.emvco.com](http://www.emvco.com)).

### **Terminal Architecture for PSAM Applications (TAPA)**

This specification is an implementation of 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 4.5.

TAPA defines the structure of a terminal as a number of handlers and devices 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 Europay, Visa and PBS.

### **Relationships between Involved Documents**

The main standards and specifications relevant for OTRS are shown in figure 4.1 where the documents named TAPA are the common documents for the open terminal architecture.

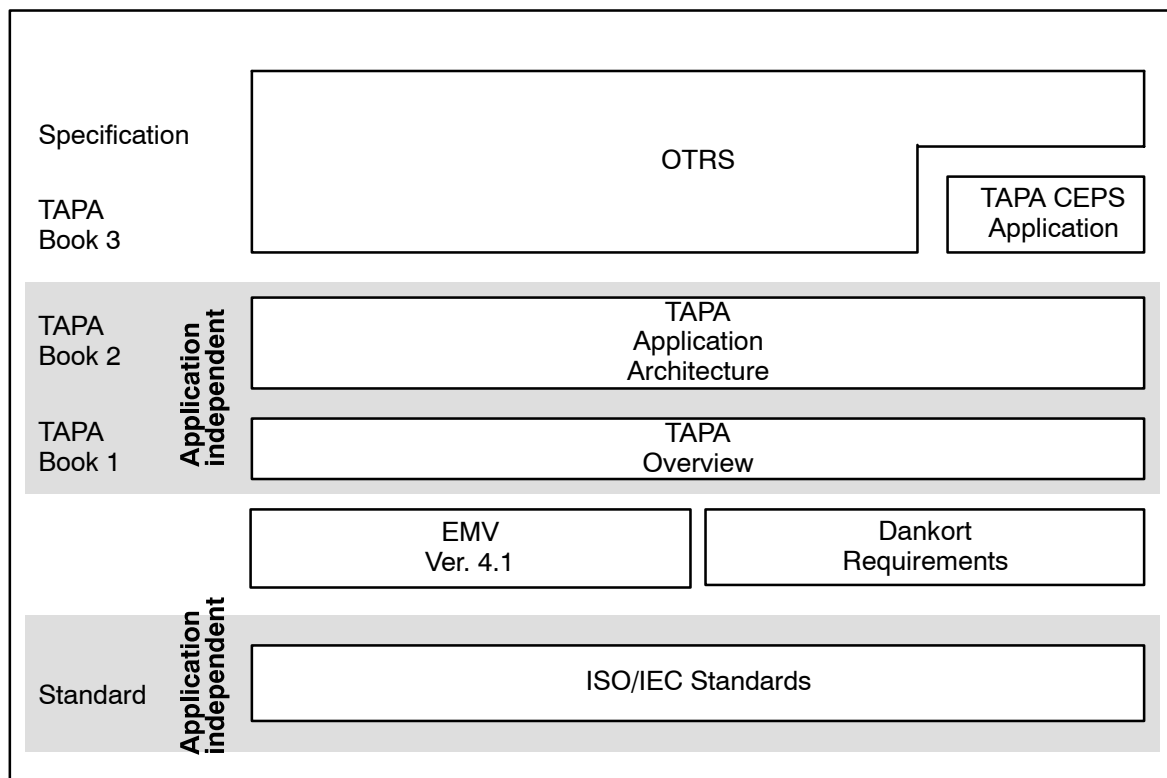


Figure 4.1 – Document Overview

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

The Dankort requirements are PBS specific and are not dealt with in any TAPA document. These functional requirements are included in this specification.

The TAPA specifications are divided into two categories, one covering the application independent terminal requirements and interfaces (books 1 and 2) and a number of application-specific specifications (book 3s) where the individual application requirements and the usage of the PSAM are specified.

This OTRS specification is based on all the documents mentioned above and covers the functions not specified in the current TAPA documents as well as proprietary functions.

### 4.2.3 Technology

#### Data Communication

Advances in communication technology allows for higher transmission speeds compared to the existing systems. Consequently, longer and more flexible messages (as required for chip card transactions) can be transmitted in the same time as the highly optimized and inflexible messages previously used.



## **Data Storage**

EEPROM technology and Flash–PROM technology makes it feasible to store transaction data in the terminal for card transactions performed offline. These transactions can be transmitted later to the host system either as individual transactions or as a batch transfer.

## **Cryptography**

Chip cards with coprocessors for cryptographic functions make it feasible to include public key technology in chip card transactions.

Advances in crypto analysis and raw computer performance for attacking crypto systems have forced the international card schemes to require the use of triple DES (3DES) and double length DES keys to be used everywhere.

### **4.2.4 Danish Regulations**

#### **Basic Regulations**

All terminal operation within the Danish banking system must comply with certain regulations as set up by the Danish Banking Association and Danish legislation. These regulations form the basis for several requirements especially when handling 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 new 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. 49: “Dankort–håndbogen” which sets up requirements, especially for the handling of PINs.

The requirements in the Dankort Handbook 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.

#### 4.2.5 Operational Regulations

Finally, the operating regulations and terminal requirements from the international card schemes, e.g. JCB, MasterCard and Visa, shall be addressed, as a given OTRS terminal shall be able to accept all card schemes from a technical point of view.

### 4.3 Business Requirements

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 basic type of terminal built from this specification containing a debit/credit application.

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

Another distinction between terminal types is the environment in which the terminal shall operate, i.e. attended, or unattended.

#### 4.3.1 Major Requirements

This section lists the most important business requirements to the OTRS terminal.

##### General Requirements

- The terminal must comply with existing standards and specifications to have the highest degree of synergy with similar projects in other countries.
- This specification must be open to all terminal manufacturer to encourage several implementations.
- Wherever applicable, flexibility must be placed in the PSAM to allow changes to the system behavior to be controlled by the Terminal Operator.
- The terminal architecture must allow other applications, such as loyalty schemes, to reside in the same terminal as the payment applications defined in this specification.
- The terminal must be equipped with a chip card reader.
- The cardholder must as default physically handle the card by himself/herself. Only special circumstances should require the card to be handled by the merchant.

- The terminal must be able to handle multiple currencies, e.g. DKK, Euro, and other currencies accepted locally.
- The terminal must at least support Danish for cardholder and merchant guidance but more languages may also be supported.

#### **Requirements specific to the Debit/Credit Application**

- The terminal must be equipped with a magnetic stripe card reader in addition to the chip card reader.
- As fallback, the card number and other data may be key entered.
- The terminal must contain a secure PIN Pad for cardholder verification. This PIN Pad is used for both magnetic stripe cards and chip cards.
- It must be possible to use signature for cardholder verification.
- This specification also enables the implementation of terminals not using any cardholder verification. The usage of such terminals is highly restricted and requires a special agreement with PBS A/S and Dankort A/S.
- The terminal must be able to establish online connection to one or more Terminal Operator(s) for certain transactions while other transactions are performed offline with later transfer of transaction data.
- The PSAM must protect all sensitive transaction data by use of enciphering and MAC'ing functions. Examples of sensitive data are the PIN and card number (PAN).
- It must be possible to set parameters for transaction handling that are individual from one merchant to another.

## **4.4 Terminal Types**

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

### **The Mail Order and Phone Order Environment**

The mail order and phone order environments are usually based on the keying of the card number and expiry date and need not support chip capabilities.

The signature from the mail order entry form is kept on file.

### **Cardholder Activated Terminals (CAT)**

The cardholder activated terminals may have different capabilities and requirements depending on the actual environment and terminal.

Different requirements are to be complied for, with the different unattended terminals. A full description is provided in Attachment E.

### **Restaurants, Hotels and Car Rentals**

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, based on the card authorization done at check-in/pick-up.

### **Fuel Dispensers**

A payment transaction at a fuel dispenser consists of two phases. First, the card is pre-authorized using an estimated transaction amount. If this completes successfully, the pump is opened for fuelling.

When fuelling is over, the exact transaction amount is now known, and the actual payment transaction is generated based on card data stored when performing the authorization. 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 residing in bank branches.

## 4.4.1 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 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 4.7.1.

### Terminal Operator

The Terminal Operator controls one or more PSAMs 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 or JCB.

### **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 PBS in each case.

### **Basic Interconnections**

As depicted in figure 4.2, the scope for this specification and the environment in which the terminal will operate is limited to defining the requirements to be met when PBS is the Terminal Operator. Depending on the card type, PBS may additionally be acquirer and possibly also card issuer or act on behalf of an acquirer and card issuer).

The terminal may contact Terminal Operators other than PBS for other applications (not involving the PBS PSAM).

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

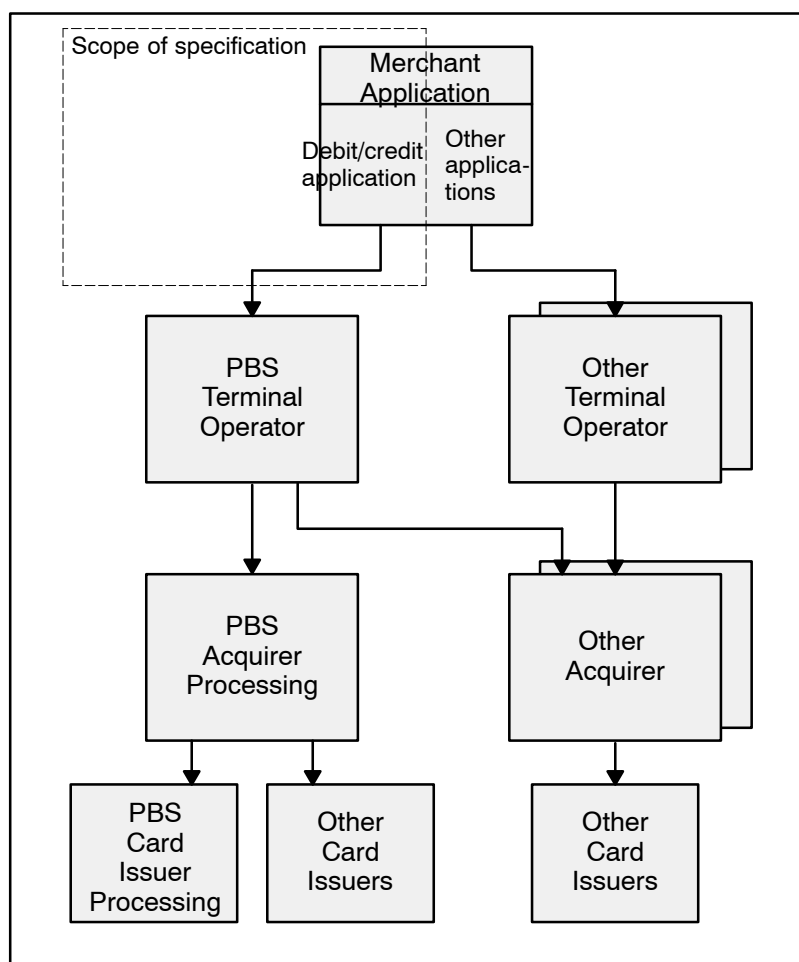


Figure 4.2 – Network Model, Debit/Credit

## 4.5 Terminal Model

This section contains more technical oriented descriptions and the term Integrated Circuit Card (abbreviated as either ICC or IC Card) will be used in addition to “chip card” to use the same term as in the remaining part of this specification.

### 4.5.1 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 4.3.

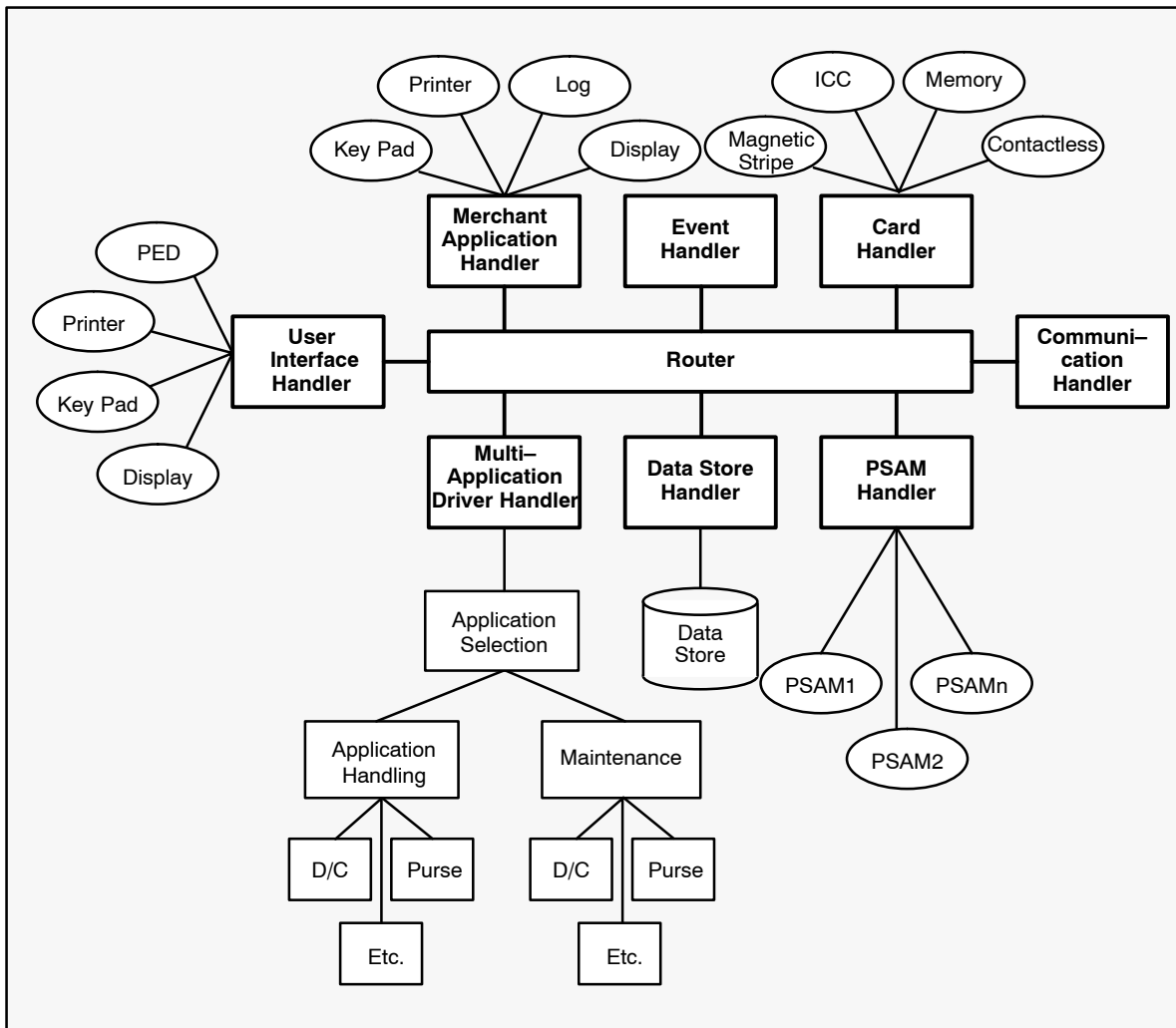


Figure 4.3 – Terminal Architecture for PSAM Applications (TAPA)

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 PBS 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 PSAM is developed by PBS as Terminal Operator.

## **4.5.2 A Physical Implementation of the TAPA Model**

Figure 4.4 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 Tamper Evident Device, and except for the PSAMs, the remaining handlers and devices constitute what is called the CAD (Card Accepting Device).

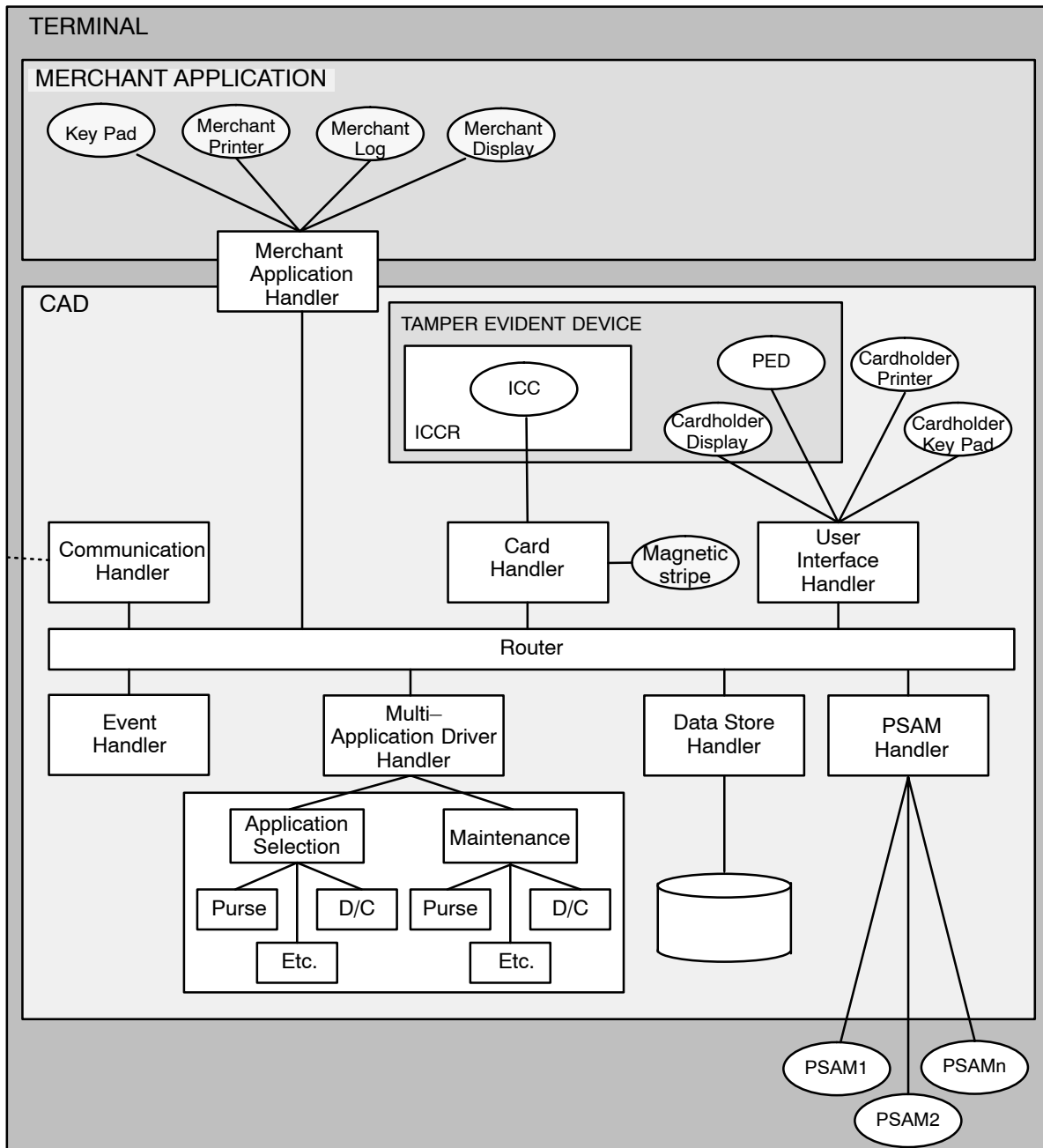


Figure 4.4 – Example of a Physical Implementation

### 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.

Furthermore, the Merchant Application may have user interfaces of no direct importance to the payment functions such as signal lamps and activation keys or handles specific for the purpose of the terminal.

If the terminal is attended, the Merchant Application shall contain a merchant display to guide the merchant.

### **The MAD–Handler**

The terminal specified will be able to handle credit and debit cards. Debit and credit cards may 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 may also be validated online. The ICC and the PIN may, 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.

### **Card Readers (General)**

The card readers for magnetic stripe cards and chip cards should preferably be combined but may 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

Unattended terminals shall, however, have a combined card reader.

If the card reader is motorized, the card may be retained in the terminal at the card issuer’s request.

### **Magnetic Stripe Card Reader**

The magnetic stripe card reader (MSCR) must as a minimum be capable of reading the ISO–defined track 2 of the magnetic stripe.

### **Integrated Circuit Card Reader**

The ICC Reader (ICCR) may be designed as either a manually operated reader or a motorized reader. If the ICCR is not integrated with the PED, it shall be housed in an Interface Device which shall be a Tamper Evident Device with cryptographic functions.

The ICCR must be capable of resetting and communicating with ICCs according to the requirements in ref. 36: “EMV, version 4.1”.

## **PIN Entry Device (PED)**

The PED is a tamper responsive device used to enter the PIN. The PIN is enciphered and sent to the PSAM which either sends it online 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.

## **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, e.g. transaction amount.

Standardized text strings allow the same cardholder dialogue in terminals from different Terminal Suppliers.

For attended terminals, a merchant display may give user guidance to the merchant and may allow him to follow the transaction progress.

The transaction result is shown in both display types.

## **Receipt Printer**

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. For each transaction initiated, a receipt shall be printed, even if the transaction was rejected or failed.

When using a CAT terminal, the cardholder may have the option to deselect the receipt.

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.

## **Command Keys**

The main purpose of the command keys is to enable the cardholder to interact with the terminal.

At least two keys shall be implemented: ACCEPT and CANCEL. It is highly recommended that a CLEAR key is also implemented.

The three keys, ACCEPT, CANCEL and CLEAR, may be contained in the PIN Pad or tamper evident area.

For the CAT only: If 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.

## **Data Store**

Transaction data created by the PSAM for debit/credit card transactions is stored in the Data Store. The MAD-Handler may also use the Data Store for its own purposes.

## **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 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 may 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.

## **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, along with the next online transaction. The stored messages will be sent after the request, that initiated the online session, has been sent to the Terminal Operator. This transfer may continue until there are no more messages to be sent or until the response to the request has been received.

The Terminal Operator will acknowledge each message received.

## **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 PBS PSAM creates the transactions and performs the security analysis of the responses received from the PBS host system.

The PBS 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 certificates for the card schemes for which PBS 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 PBS PSAM, the online PIN will be decrypted and re-encrypted using a dedicated online PIN encryption key. The offline PIN may 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 PBS 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.

### 4.5.3 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 4.5, input to the MAD-Handler application selection may 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.

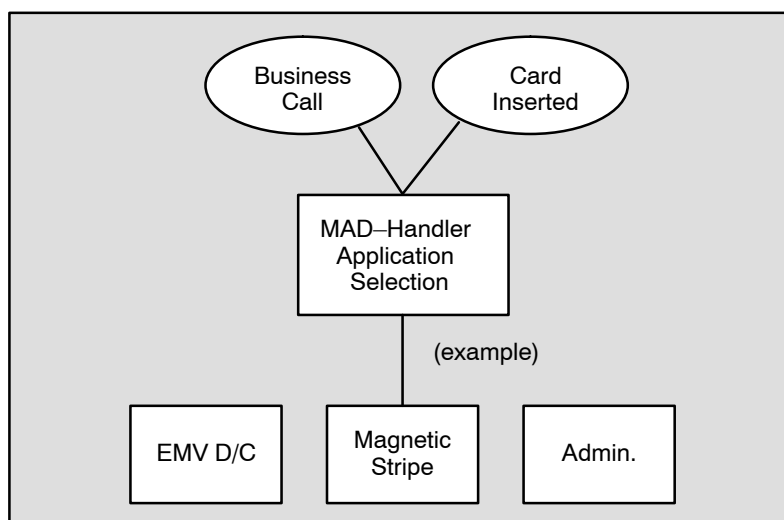


Figure 4.5 – Application Selection Principle (Example)

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, sometimes after a dialogue with the cardholder.

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.

## 4.6 Transaction Types

This section lists the various transaction types that are defined for the debit/credit applications. The transaction types are further separated into card related transactions and administrative transactions.

### 4.6.1 Card Related Transactions for the Debit/Credit Application

The Merchant Application can initiate the transactions described in this section. Although they are always related to a given debit/credit card, the card may not always be physically involved in the transaction.

Transactions are either handled offline by the MAD–Handler and PSAM or may additionally result in an online connection with an acquirer via the Terminal Operator. Depending on the card type, the transaction may be forwarded to the card issuer.

The following transactions are defined:

- Purchase
- Authorization (Original or Supplementary)
- Capture
- Reversal (Authorization)
- Refund

#### **Purchase**

The Purchase transaction 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 transaction may be performed offline or online.

**NOTE:** 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 only possible if allowed by the acquirer and card issuer.

#### **Original Authorization/Supplementary 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. 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 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 Capture transaction may 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.

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).

**NOTE:** The card is not involved for the Supplementary Authorization transaction as all necessary information is stored in the Token.

### **Capture**

This transaction type requires a Token as input. Based on the previously authorized amount(s) (stored in the Token), the PSAM generates a transaction that is stored in the terminal for later transmission to the acquirer.

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

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

### **Reversal (Authorization)**

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) transaction may be initiated. The purpose of this is to adjust the cardholder's spending limit in the issuer system.

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

**NOTE:** 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.

### **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.

#### **4.6.2 Administrative Processes for the Debit/Credit Application**

The Merchant Application can initiate the following administrative processes:

- Installation
- Advice Transfer
- PSAM Update
- PSAM Deactivation

##### **Installation**

The Installation process is used when a new PSAM is inserted in an existing terminal and when a PSAM is inserted in a new terminal. The Installation process starts by a request to the PSAM for generating an Installation Transaction message. This message is sent as an online message to the Terminal Operator. This process is normally followed by the PSAM Update process to ensure that the new PSAM has all current data needed to perform transactions.

##### **Advice Transfer**

The Advice Transfer is an administrative process which is performed online with the acquirer via the Terminal Operator. During Advice Transfer, the terminal will send all stored advices to the Terminal Operator. Normally, the Advice Transfer will be followed by a PSAM Update process to ensure that the PSAM always has all current data needed to perform transactions.

##### **PSAM Update**

The PSAM Update process starts by an online request to the Terminal Operator to send any pending updates of data elements for a given PSAM. Each of these updates are then sent by the Terminal Operator and acknowledged by the terminal after temporarily storing them. After disconnecting the communication link, the updates are sent to the relevant PSAM.

##### **PSAM Deactivation**

The PSAM Deactivation transaction is very critical online transaction as it irreversibly puts the PSAM out of function. The purpose is to effectively disable the PSAM if it shall never be used again. This may be relevant in case a merchant cancels the contract with the Terminal Operator/acquirer or in the case of a physical PSAM upgrade where the old PSAM has to be returned to the Terminal Operator.

### 4.6.3 Transaction and Message Flow, Debit/Credit

#### Online

The terminal will process a card in a purchase situation as follows:

- The card is read in the chip card reader or in the magnetic stripe card reader,
- The application in the chip card is selected by the cardholder and activated,
- The relevant applications in the terminal and PSAM are activated based on the business call and the card inserted,
- The application activated in the card is validated by the applications in the terminal and the PSAM.

Following a successful activation and validation of the application in the chip card, the terminal performs Terminal Risk Management and Analysis. Together with the Card Action Analysis the combined result determines whether an entered PIN shall be verified online by the acquirer/issuer or offline by the card itself. Regardless of whether the PIN is processed online or offline, a transaction is created and sent via the Terminal Operator to the acquirer/issuer for further processing.

The transaction is verified by the acquirer and/or issuer who, after processing the transaction, sends a response to the terminal indicating whether the transaction was successful or not.

#### Offline

If the transaction is requested to be performed offline, the terminal will first check whether offline processing of the selected application in the card is allowed.

Transactions based on the magnetic stripe of a card are as default always performed online with the acquirer/issuer. Only in very specific and exceptional situations will it be allowed to perform an offline transaction based on a magnetic stripe.

Although the terminal may be capable of handling off-line transactions, branding rules must be observed, i.e. certain card products cannot be handled offline.

If offline processing is performed, the application in the card is statically/dynamically authenticated, if possible, by the application in the terminal and PSAM. Cardholder Verification Method (CVM) will be offline PIN, signature or none. When the application in the card has been authenticated and CVM was successfully performed, the transaction is generated and stored in the terminal, including the transaction certificate generated by card. Whenever possible, offline generated transactions are transmitted to the Terminal Operator.

### **Fallback to Offline**

If the Terminal Operator could not be reached by the terminal, e.g. because of communication problems, the transaction may be performed offline according to the parameters in the terminal application and Service Codes on the card.

### **Fallback to Magnetic Stripe**

If the ICC failed e.g. due to communication error, fallback to the magnetic stripe must be done. A transaction performed on the basis of fallback to magnetic stripe must go online with the acquirer/issuer as specified by the individual card schemes.

### **Fallback to Key Entered Card Number**

If the magnetic stripe could not be read, fallback to manually keying in the card number and expiry date may be done.

### **Transaction Result**

A transaction can end in the following ways:

- Approved
- Referred
- Declined
- Failed

Approved transactions are successful and the services/goods can be rendered if applicable.

Referred transactions require additional action performed by the merchant, e.g. making a phone call to the issuer's or acquirer's helpdesk.

Transactions can be declined by either the terminal, the PSAM, the Terminal Operator, the acquirer or the issuer. Examples are that the card is not accepted in the given terminal or the transaction amount is too high. An EMV card itself may also decline a transaction, even if it has been approved by the card issuer.

Transactions can fail due to technical problems, e.g. it was not possible to establish an online connection to the Terminal Operator or the transaction timed out.

## 4.7 Security

### 4.7.1 Security Zones, Debit/Credit

The terminal being specified is seen as a basic element in the infrastructure for card transactions in which PBS takes part. Consequently, the security requirements are those fulfilling the security level required by PBS and its cooperating partners.

The PIN Entry Device (PED) or PIN Pad and the PBS 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 4.6, one PSAM (PSAM 1) is controlling the security zones between the PSAM and the PED 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.

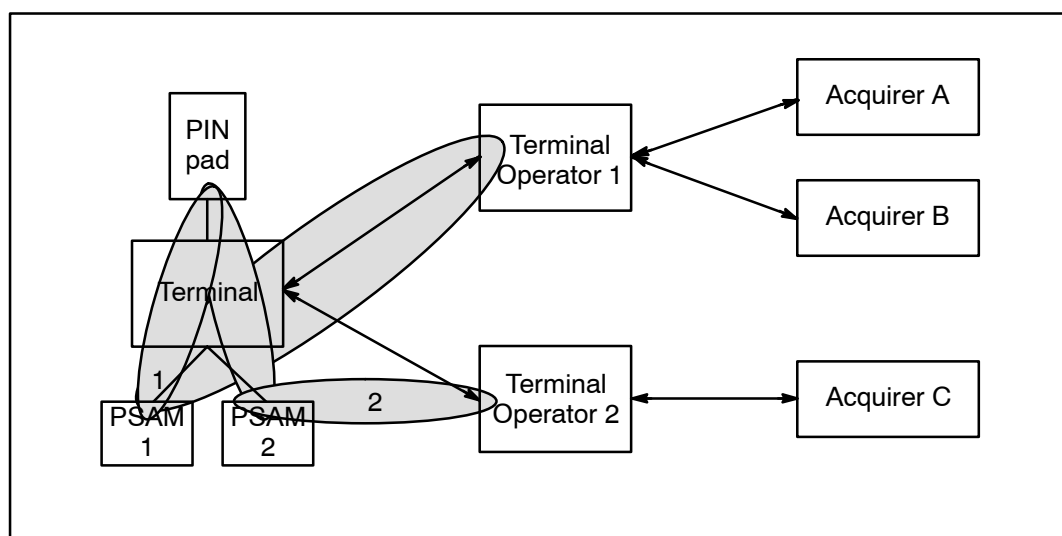


Figure 4.6 – Security Zones in an Open Terminal Environment

When another application needs to have a PIN validated, the PSAM (PSAM 2) does not share the security zone 1 because of the possibility of having the PIN sent to the wrong Terminal Operator together with the information in 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.

## 4.8 Developing an OTRS Terminal

Any vendor is welcome to develop a terminal fulfilling the requirements, then to have the terminal certified and finally to sell it in the market.

## 4.8.1 Development Phases

### Phasing out old Terminals

The regulations from the International card schemes – Visa, MasterCard, JCB and others – require all terminals accepting cards from these card schemes to be upgraded to chip functionality by 2005. New terminals in the market must be compliant by 2001.

Although a magnetic stripe may continue to be present on the payment cards, not all card brands may continue to be accepted if the terminal is capable of handling magnetic stripe cards only.

## 4.8.2 Certification of Terminals, PEDs, and Environment

### Introduction to the Certification Process

The terminal specified in this specification shall be fully tested and the PED shall be security evaluated before the terminal is installed for operation.

The PED (PIN pad) is subject to specific procedures required by Visa and MasterCard, requirements for these approval procedures need to be followed accurately and shall be obtained from the card schemes.

Please note, that is the responsibility of the PED manufacturer to conduct the approval processes specified by Visa and MasterCard, respectively.

The increased complexity of a terminal accepting both MSC and ICC, and the inclusion of requirements like EMV, enhances the certification procedures.

The testing of the MSCR and the PSAM interface is the responsibility of PBS which uses Delta Electronics Testing as Test House for the electrical tests. The functional application testing is performed by PBS.

The ICC debit/credit testing is performed in two levels: EMV level 1 test (the physical interface) and EMV level 2 test (EMV application functionality) which both are the responsibility of the vendor and is performed by an EMVCo accredited Test House. Further functional application testing is performed according to the PBS test specification and may be performed either by PBS or by an accredited Test House.

After EMVCo has issued its approval for the EMVCo Level 2 test, further testing is required by the card schemes. Visa has a few EMV test cards which must be used for verifying the full path between the ICC and the Visa systems. MasterCard has a TIP test which has to be performed at an accredited Test House, e.g. PBS. The MasterCard test is mandatory for all terminals

and integrations with ECRs. Also, JCB have test suites to perform and report the results, American Express etc..

It is the responsibility of the terminal manufacturer to ensure that the terminal has passed all approvals before installing it for operation at the merchants.

If the terminal is an integrated part of a shop system, e.g. a cash register, the test will include such back-office equipment as well.

It is the responsibility of the terminal manufacturer to enter the necessary agreements with the selected Test House(s) and to provide the test reports to PBS before functional testing can be performed. Some tests may be performed in parallel, though. Possibly more Test Houses will be able to perform the complete testing.

For further description and actual requirements regarding the terminal and PED certification procedures, see Attachment D: “Certification”.

### **Procedure for obtaining waivers**

During the development of a terminal implementation of OTRS it may prove necessary to obtain waiver(s) for specific OTRS requirements.

Waivers may be obtained for B- and C-requirements while the vendor cannot expect a waiver for an A-requirement.

Any application for a waiver must be substantiated and an alternative solution which fulfills the background for the requirement must be described if relevant. The template for applying for a waiver can be found in ref. 48: “Technical Reference Guide – OTRS Test Specification”.

This page is intentionally left blank



# 5. Application-independent Requirements

## 5.1 Introduction

This chapter contains requirements that are common to all terminal applications, irrespective of the card types accepted.

Application-specific requirements for the debit/credit application is defined in chapters 6.

*Functional* requirements are defined in this chapter whereas *design* requirements are defined in chapter 10.

### 5.1.1 Terminal Profiles

The Terminal Supplier must decide which functionality should be implemented.

- |         |   |  |
|---------|---|--|
| 5.1.1.1 | A | The terminal shall be capable of handling debit/credit cards   |
| 5.1.1.2 | B | If debit/credit cards are supported, <i>both</i> IC Cards and magnetic stripe cards shall be supported.  |
| 5.1.1.3 | A | The terminal shall be either: <ul style="list-style-type: none"> <li>• Attended, or</li> <li>• Unattended (Cardholder Activated Terminal, CAT).</li> </ul> |

**NOTE:** See Attachment E for definition of CAT levels, i.e. different types of unattended terminals.

In certain environments, terminals may be attended some of the time, while left unattended the rest of the time.

### 5.1.2 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. 40: “TAPA, Application Architecture Specification”.

- |         |   |  |
|---------|---|--|
| 5.1.2.1 | A | Except when specifically stated, the terminal shall comply with ref. 40: “TAPA, Application Architecture Specification”. |
|---------|---|--|

**NOTE:** This common architecture allows implementation on top of existing terminal architectures such as OTA, OPT, ITA, STIP, etc.

- 5.1.2.2 A The terminal shall comply with ref. 36: “EMV, version 4.1” and related bulletins issued by EMVCo.

**NOTE:** As EMV is “non-forgiving” and “non-waivered”, all mandatory terminal related requirements in ref. 36: “EMV, version 4.1” 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.

- 5.1.2.3 A Furthermore, the terminal shall comply with the terminal specifications as issued by card schemes, e.g. ref. 43: “Visa Integrated Circuit Card. Terminal Specification” and ref. 44: “Terminal Requirements for Acceptance of Chip Pay Now (Debit) and Pay Later (Credit) Cards”.

**NOTE:** The card schemes defines 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 3.6, “Related Websites”.

#### Card Specification

- 5.1.2.4 A The terminal shall accept cards complying with ref. 36: “EMV, version 4.1” if capable of performing debit/credit transactions.

### 5.1.3 Documentation

Due to the complexity of a terminal capable of handling the full set of functions defined in this specification, two explicit requirements shall be fulfilled by the Terminal Supplier:

- 5.1.3.1 B A Quality Handbook of the Terminal Supplier shall be delivered to PBS.
- 5.1.3.2 B A Security Handbook of the Terminal Supplier shall be delivered to PBS.

### 5.1.4 Patent Issues

- 5.1.4.1 A The Terminal Supplier shall make the necessary arrangements with any patent holder holding a patent which may be infringed by designing and constructing terminals according to this specification.

## 5.2 General Requirements

### 5.2.1 Protected Functions

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.

- 5.2.1.1 B The terminal shall 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.
- 5.2.1.2 B The 'lock' function shall be managed by the merchant and the 'lock' function shall allow the merchant to authorize clerks individually.
- 5.2.1.3 B The 'lock' function shall be implemented as part of the Merchant Application.
- 5.2.1.4 B The Refund transaction shall be protected by a 'lock' function, to ensure that only authorized clerks will be able to initiate Refund transactions

### 5.2.2 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).

- 5.2.2.1 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.
- 5.2.2.2 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.
- 5.2.2.3 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'.
- 5.2.2.4 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'.

## 5.3 The Router

The Router controls all communication between the individual handlers in the terminal.

### 5.3.1 Functional Requirements

- 5.3.1.1 A The Router shall conform to the requirements in ref. 40: “TAPA, Application Architecture Specification”, section 4.1.

### 5.3.2 Exception Handling

- 5.3.2.1 B The Router shall be able to resolve dead-lock situations, e.g. by implementing overall time-out mechanisms.

### 5.3.3 Command Flow

The command flow is defined in ref. 40: “TAPA, Application Architecture Specification”, section 4.2.

## 5.4 Multi-Application Driver Handler (MAD-Handler)

### 5.4.1 General Requirements

- 5.4.1.1 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.
- 5.4.1.2 A The MAD-Handler shall finish the start-up sequence for one terminal application before starting the next.
- 5.4.1.3 A The MAD-Handler shall keep track of the current cardholder dialogue, e.g. by implementing a state machine.

#### Clean Up and Guard Time

In order to minimize the processing time in the PSAM, the PSAM v.50 (and coming versions) 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 send to the PSAM immediately after the response to *Complete Payment* 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.

- 5.4.1.4 A After the response to *Complete Payment* command is received, a delay of minimum 500 milliseconds shall elapse, before any new command shall be send to the PSAM.

**NOTE:** Processing in the terminal, not involving the PSAM, shall not be influenced by this guard time.

## 5.4.2 Printing

- 5.4.2.1 A The MAD–Handler shall control all printing of cardholder receipts.

- 5.4.2.2 A If the terminal is attended, the merchant shall be able to request a copy of the previous receipt. If the previous receipt came from a signature based transaction both the merchant and the cardholder copies shall be printed.

- 5.4.2.3 C The MAD–Handler may control printing of reports, receipts, etc. for the Merchant Application.

## 5.4.3 Log

- 5.4.3.1 A The MAD–Handler shall control all logging activities except the logging of the “Advice to Log”.

- 5.4.3.2 A The MAD–Handler shall have access to a Log.

**NOTE:** The Journal/Log may be implemented as a “paper–journal” and/or electronically stored as a data file.

- 5.4.3.3 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.

- 5.4.3.4 B Entries in the Log shall be stored for a minimum of 18 months.

- 5.4.3.5 A All transactions shall be stored in the Log, irrespective of the result.

- 5.4.3.6 A If the Log is not ready to store another entry, it shall not be possible to initiate a transaction.

- 5.4.3.7 A It shall be possible to readily make a plaintext print–out or a copy of the Log.

- 5.4.3.8 A Upon request, a print–out of the Log shall either include one transaction or a sequence of transactions.

- 5.4.3.9 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.
- 5.4.3.10 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 legislation requirements.
- 5.4.3.11 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<sub>NUMBER</sub> and ID<sub>PSAM</sub>, may not be repeated for each log entry, unless the information is necessary to identify the specific terminal.
- 5.4.3.12 A The only cardholder data to be logged in plaintext is the PAN.
- NOTE:** Additional cardholder data shall be protected according to ref. 24: “Payment Card Industry Data Security Standard”.
- 5.4.3.13 A In case of one log being shared by several terminals, it shall be unambiguously stated which terminal has generated which transaction log entry.
- 5.4.3.14 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 payed for.
- 5.4.3.15 A If an error occurs during a transaction, the ASW1–ASW2 shall be printed/saved as part of the Log.

#### 5.4.4 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.

- 5.4.4.1 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.

- 5.4.4.2 A If a failure is detected in any of the components, the CAD shall end normal operation and, if possible, display the relevant error–message.
- 5.4.4.3 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.
- 5.4.4.4 A The MAD–Handler shall be able to detect ‘Out of Paper’ in the receipt printer, and stop normal operation until new paper is inserted.
- 5.4.4.5 B The MAD–Handler shall be able to detect ‘Paper Low’ in the receipt printer.
- 5.4.4.6 B 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”.
- 5.4.4.7 A The MAD–Handler shall be able to detect that a power failure has occurred during processing of a transaction.
- 5.4.4.8 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.
- 5.4.4.9 A It shall *not* be possible to initiate a transaction on an attended terminal if there is a failure or out of paper in the receipt printer.
- 5.4.4.10 A When there is a failure in the receipt printer on a CAT–terminal, an error message on the Cardholder Display indicating that a receipt cannot be printed shall be displayed, see table M.1 (Attachment M), Message Code ‘E1’.

## 5.5 Card Handler

### 5.5.1 General Requirements

- 5.5.1.1 A If the debit/credit application defined in chapter 6 is implemented, the following sub–handlers shall be implemented:
- Processor card reader
  - Magnetic stripe reader
- 5.5.1.2 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).

- 5.5.1.3 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.
- 5.5.1.4 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.

#### Card Selection

- 5.5.1.5 A Technology selection, i.e. IC or magnetic stripe, shall be done in accordance with ref. 36: “EMV, version 4.1”.
- 5.5.1.6 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 type, the application selection process can start.

### 5.5.2 Sub-handler, Magnetic Stripe Card Reader (MSCR)

#### Conformance to TAPA

- 5.5.2.1 A The MSCR shall conform to ref. 40: “TAPA, Application Architecture Specification”, section 6.1 with the following exceptions:
- Reading ISO track 1 is optional
  - Reading ISO track 3 is optional
  - Writing ISO track 3 is optional

#### Reading of ISO Track 2

**NOTE:** Technical requirements to the reading of MSCR are defined in section 10.2.4.

#### Validation of ISO Track 2

The task of the MSCR is to validate the characters read to identify reading errors. Validation of the contents of track 2 is left for the MAD-Handler which also selects the proper PSAM and PSAM application to handle the transaction.

- 5.5.2.2 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 2 has been read.



- 5.5.2.3 A The MSCR shall validate that the first character is a start sentinel (B'1011).
- 5.5.2.4 A The MSCR shall validate that the second last character is an end sentinel (B'1111).
- 5.5.2.5 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. 3: "ISO/IEC 7811–2", subclause 12.2.
- 5.5.2.6 A The MSCR shall validate that a maximum of 40 data characters are read from track 2 (including the start and end sentinels, the control characters and the longitudinal redundancy check character).
- 5.5.2.7 C The MSCR may be able to buffer up to 40 characters read from track 2 (the entire track).
- 5.5.2.8 A The MSCR shall be able to buffer the 37 characters that may be requested from other handlers in the CAD. These characters constitute the entire track 2 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").
- 5.5.2.9 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 the validation of the check digit in the PAN (Luhn–digit) and shall therefore not be considered as one of the validations mentioned above.
- 5.5.2.10 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 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.
- 5.5.2.11 B If a Card is swiped through the reader while a transaction is in progress, the terminal shall cancel the current transaction unless the cardholder has pressed the "ACCEPT" button.
- 5.5.2.12 A If the "SLET ALT" (Cancel) key has been pressed and the the card is retained in a motorized– or locking card reader, the card shall be returned immediately unless the cardholder has pressed the "ACCEPT" button.

### 5.5.3 Sub–handler, ICCR – General

- 5.5.3.1 A The ICCR shall comply with ref. 36: "EMV, version 4.1".

### Repeat Last ICC Response

- 5.5.3.2 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<sub>DATA</sub>
  - Card Response
  - Response Code

- 5.5.3.3 A When the Card Handler receives a *Repeat Last ICC Response* command, the response shall contain the data elements previously stored (see requirement 5.5.3.2)

The format of the *Repeat Last ICC Response* command can be found in section 8.6.22.

## 5.5.4 Sub-handler, ICCR – Processor Card Reader

### General Requirements

- 5.5.4.1 A The Processor Card Reader shall always be aware, whether a Processor Card is present or not.
- 5.5.4.2 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 the behalf of the Processor Card using the proper Response Code.
- 5.5.4.3 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.

- 5.5.4.4 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

- 5.5.4.5 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. 40: “TAPA Application Architecture Specification”.

## 5.5.5 Interface to the Processor Card

### Establishing Communication with the Processor Card

- 5.5.5.1 A The Processor Card Reader shall be able to establish communication with the Processor Card according to the requirements specified in ref. 36: “EMV, version 4.1” (both the transport protocols T=0 and T=1 are mandatory for the terminal).

### Protocol and Parameter Selection (PPS)

- 5.5.5.2 B The Processor Card Reader shall be able to participate in a Protocol and Parameter Selection dialogue with the Processor Card.

**NOTE:** Even though the present version of the EMV specification does not support PPS, it is stated that future versions of the specification may require the terminals to support the PPS.

- 5.5.5.3 A If the Protocol and Parameter Selection dialogue is implemented, it shall comply with ref. 8: “ISO/IEC 7816–3”.

## 5.6 User Interface Handler

### 5.6.1 Sub–handler, PIN Pad

#### Introduction

- 5.6.1.1 A The PIN Pad shall fulfil all PIN Pad related requirements defined in ref. 40: “TAPA, Application Architecture Specification”.

Additional functional requirements are defined below.

A number of design requirements defined in Chapter 10 must be fulfilled as well.

- 5.6.1.2 A The procedures for security evaluation and audit of key loading as defined in Attachment D 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

- 5.6.1.3 A All systems and equipment shall comply with the requirements for PIN management and security as defined in ref. 16: “ISO 9564-1”.
- 5.6.1.4 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.
- 5.6.1.5 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.
- 5.6.1.6 A All internal circuits and connections within the PIN Pad shall be highly physically protected and thereby prohibit tapping.
- 5.6.1.7 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.
- 5.6.1.8 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 re-formatting is handled by the PSAM.
- 5.6.1.9 A PIN data shall be deleted when returned in the response to the *Get PIN* command or upon a time-out condition.
- 5.6.1.10 A The software shall be designed in such a way that its intended functions cannot be misused or circumvented from the outside world.
- 5.6.1.11 A The PIN Pad shall not be operational until the PIN Pad ID and related keys have been loaded.

### Packaging

- 5.6.1.12 A As defined in ref. 40: “TAPA, Application Architecture Specification”, the PIN Pad shall be part of a Tamper Evident Device, also housing the ICCR and the Cardholder Display.
- 5.6.1.13 C The Tamper Evident Device may optionally house the full CAD implementation.

### PIN Pad Keyboard

- 5.6.1.14 A The PIN Pad shall contain a key for each of the 10 possible PIN digits (0-9).
- 5.6.1.15 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 5.1.

Table 5.1 – 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. 16: “ISO 9564–1” and ref. 17: “ISO 9564–2”, may be used as synonyms for decimal digits. Further guidance is given in ref. 16: “ISO 9564–1”, annex F.

- 5.6.1.16 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 “GODKEND” (Enter/ Accept) key.

- 5.6.1.17 A Any input shall be confirmed by pressing the validation key “Enter”.
- 5.6.1.18 A There shall be a separate command key to cancel or correct the PIN entry.
- 5.6.1.19 A A visible signal shall indicate data entry and shall be independent of the actual key being pressed.
- 5.6.1.20 A A PIN Pad shall support entry of a four (4) to twelve (12) digits PIN.
- 5.6.1.21 A Only a fixed symbol, such as the ‘\*’ character, shall be displayed for each PIN digit entered.
- 5.6.1.22 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.
- 5.6.1.23 A If the amount is entered on the same key pad as the PIN, the amount shall be validated before PIN entry is allowed.

- 5.6.1.24 A The first digit of the PIN to be entered shall be the high-order digit.

### Local PIN Verification

Other cards (not acquired by PBS) with PIN may have the PIN checked by the PSAM/PIN Pad. For more details, see Attachment P, “Local PIN”.

## 5.6.2 Sub-handler, Printer

### Receipts

- 5.6.2.1 A The User Interface printer shall at least support printing of the receipts defined in Attachment G.

## 5.6.3 Sub-handler, Cardholder Key Pad

- 5.6.3.1 B The command keys “SLET ALT” and “GODKEND” listed in table 5.2 shall be implemented on the Cardholder Keyboard.

**NOTE:** The “SLET” (Clear) key may be omitted.

Table 5.2 – Command keys

Key	Functionality
“SLET ALT” (Cancel)	Used for cancelling the transaction in progress.
“SLET” (Clear)	Used for clearing entered PIN digits.
“GODKEND” (Accept)	Used for accepting the Amount.

- 5.6.3.2 B If keys other than the command keys listed in table 5.2 are implemented on the Cardholder Keyboard, they shall be different in size, shape and color and shall not be mounted together with the command keys.

**NOTE:** Requirement 5.6.3.2 does not apply for the “Info” key. See section 10.2.10, page 10–16.

## 5.6.4 Sub-handler, Cardholder Display

A number of “standard” display texts for guiding the cardholder are defined in table M.1. Each display text is given a message identifier according to ref. 36: “EMV, version 4.1”.

### General display requirements

- 5.6.4.1 A The Cardholder Display shall always react on a cardholder action, e.g. when the cardholder presses the Cancel button.

- 5.6.4.2 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.
- 5.6.4.3 B If alternating text is used, every sequence of the alternating text shall be displayed for at least 1 second.
- 5.6.4.4 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.
- 5.6.4.5 A Error messages shall be displayed for at least 6 seconds or until the cardholder has performed the appropriate action.
- 5.6.4.6 C Essential information, e.g. Amount, may be emphasized on the display, e.g. by using bold characters or a bigger font.
- 5.6.4.7 A When the Currency Code is displayed, it shall be displayed in the corresponding alpha-characters according to ref. 15: “ISO/IEC 8859–15”.

### 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 10.2.7.

- 5.6.4.8 A If the Cardholder Display cannot display 4 lines of 20 characters, the display texts shall be edited in cooperation with PBS.
- 5.6.4.9 A If the Cardholder Display supports 4 lines of 20 characters, the display texts shall be as stated in table M.1.
- 5.6.4.10 B The Danish version of the display texts in table M.1 shall be used.
- 5.6.4.11 C Languages other than Danish may also be supported.
- 5.6.4.12 A If languages other than Danish are supported, English shall also be supported.
- 5.6.4.13 A If languages other than Danish are supported, the English version of the display texts in table M.1 shall be used when the terminal is displaying English texts.
- 5.6.4.14 A If display texts in a language different from Danish and English are used, the display texts shall give the same information as the Danish texts stated in table M.1.

The display messages has a number (EMV message identifier) according to the standard messages defined in ref. 36: “EMV, version 4.1”.

Definition of Message Codes are assigned according to table 5.3.

Table 5.3 – 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 Attachment M: “Guidelines for Usage of the User Interface Display” and section 6.7 “User Interface Handler” for further details.

### 5.6.5 Sub-handler, Audio Indicator

The audio indicator helps the cardholder to find out whether a transaction was approved or rejected. The design requirements for the audio indicator can be found in section 10.2.8.

The following requirements defines which events that shall initiate an audio signal.

- 5.6.5.1 B An audio indicator shall emit a signal in order to indicate that the transaction is completed successfully.
- 5.6.5.2 B An audio indicator shall emit a signal in order to indicate that the transaction is failed/rejected.
- 5.6.5.3 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.
- 5.6.5.4 B If the volume of the audio indicator is adjustable, a separate volume control shall be implemented when indicating card not removed, see requirement 5.6.5.3.
- 5.6.5.5 C The audio indicator may also signal other events e.g. when depressing numeric or function keys.



## 5.7 Merchant Application Handler

### 5.7.1 Sub-handler, Log

- 5.7.1.1 A The Log shall support all log activities.

### 5.7.2 Sub-handler, Serial Ports

This sub-handler need not be implemented to support the applications defined in this specification.

### 5.7.3 Interface between CAD and Merchant Application

The actual implementation of this interface is outside the scope of this specification. However, the following requirements shall be taken into account:

- 5.7.3.1 A The protocol defined for the interface between the CAD and the Merchant Application shall ensure that both parts have a consistent knowledge of actual transaction step and the final transaction result.
- 5.7.3.2 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.

## 5.8 PSAM Handler

### 5.8.1 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.

#### Transmission Protocol (T=1)

- 5.8.1.1 A The PSAM Handler shall be able to communicate with the PSAM using the T=1 protocol, as described in ref. 8: “ISO/IEC 7816–3”.

### Protocol and Parameter Selection (PPS)

- 5.8.1.2 B The PSAM Handler shall be able to participate in a Protocol and Parameter Selection dialogue with the PSAM as defined in ref. 8: “ISO/IEC 7816-3”.

**NOTE:** The PPS procedure shall be performed immediately after analyzing the ATR and before sending any I, R or S-blocks.

### 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 interface device (terminal).

- 5.8.1.3 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.

**NOTE:** The information field size for the PSAM (IFSC) is given in the Answer-to-Reset, see table 5.4.

- 5.8.1.4 B Consequently, the first block sent by the terminal following the PPS (if performed) shall be an S(IFS request) with IFSD = 254.

## 5.8.2 EMV Compatibility of the PSAM Interface

### Introduction

As the interface to the PSAM(s) is defined in ref. 8: “ISO/IEC 7816-3”, an existing implementation of an EMV compliant interface will not fulfill all the requirements to be complied to according to this specification.

The following section describes the changes necessary to make an EMV compliant interface useable for a PSAM.

### Handling the ATR (T=1)

The ATR from the PSAM contains the characters defined in table 5.4.

**NOTE:** The values given in table 5.4 are subject to changes and may be changed without further notice.

Table 5.4 – PSAM ATR

Character	Definition	Codes	Value	EMV Compatible
TS	Initial Character		'3B'	Yes
T0	Format Character	Y(1) and K (number of Historical Characters)	'BK'	Yes <sup>1)</sup>

TA1	Interface Character	FI and DI	'18'	No <sup>2)</sup>
TB1	Interface Character	PI and II	'00'	Yes
TC1	Interface Character	Extra guardtime	–	Yes <sup>3)</sup>
TD1	Interface Character	Y(2) and T	'81'	Yes
TD2	Interface Character	Y(3) and T	'31'	Yes
TA3	Interface Character	IFSC	'FE'	Yes
TB3	Interface Character	BWI and CWI	'64'	No <sup>4)</sup>
T1..TK	Historical Characters		'zz'..'yy'	Yes
TCK	Check Character		'XX'	Yes

**Legend:**

- 1) The terminal shall accept all values if the content of the ATR is consistent.
- 2) TA1 is allowed if the terminal is able to support the indicated mode. The PSAM interface needs to implement PPS to switch to higher communication speed.
- 3) The terminal shall accept an ATR not containing TC1.
- 4) The terminal shall accept and be capable of using the values defined in ref. 8: "ISO/IEC 7816–3".

**Cold/warm Reset**

The PSAM interface need not support the EMV cold/warm reset mechanism as the PSAM uses the PPS procedure for setting the communication speed.

**NOTE:** The current PSAM is capable of communicating with a baud rate up to 115.200. The terminal should negotiate as high a baud rate as possible to increase the overall transaction speed.

**Power Supply**

The current PSAM platform will consume 20 mA when idle. This is within the specification for an EMV compliant card reader.

**Waiting Time Extension (WTX)**

The Waiting Time Extension mechanism is supported in the EMV specification and need be implemented.

**Other Remarks**

The EMV specification does not support I–blocks with a length of 0 bytes.

### 5.8.3 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 to obey the transmission protocol. Likewise, responses from other handlers to the PSAM are embedded in special commands.

- 5.8.3.1      A      The CAD shall in addition to the TAPA defined commands, support the commands defined in table 8.1 as necessary for the applications supported (debit/credit).

## 5.9 Data Store Handler

### 5.9.1 Sub-handler, 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.

- 5.9.1.1 A The Data Store Handler shall comply with ref. 40: “TAPA, Application Architecture Specification”.
- 5.9.1.2 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.
- 5.9.1.3 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:** Resetting the Data Store shall not be performed unless the Data Store is empty.
- 5.9.1.4 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.
- 5.9.1.5 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 6.18.6.
- 5.9.1.6 C The Data Store Handler may contain an error correction feature in order to recover unintended alteration in data during storage.

## 5.10 Communication Handler

### 5.10.1 General Requirements

- 5.10.1.1 A The Communication Handler shall comply with ref. 40: “TAPA, Application Architecture Specification”.

## 5.11 Event Handler

### 5.11.1 General Requirements

- 5.11.1.1 A The Event Handler shall comply with ref. 40: “TAPA, Application Architecture Specification”.

## 5.12 Terminal Initialization

This section describes the initialization process common to all applications. Initialization procedures specific for the debit/credit application is specified in chapters 6.

### 5.12.1 Reset of the CAD

- 5.12.1.1 A Initialization of the CAD shall be done automatically after power-on.
- 5.12.1.2 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.

## 5.13 Application Selection

### 5.13.1 Introduction

#### Preparation

When a card has been read by one of the card readers (MSCR or ICCR), the terminal must decide if an application in the

MAD–Handler 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 MAD–Handler requests a table for MSC selection and a table for ICC selection from each relevant application/PSAM present in the terminal.

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.

Depending on the algorithm chosen for using the tables, they may need sorting after having obtained information from all the PSAMs.

### **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.

## **5.13.2 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 entries. 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.

- 5.13.2.1 A For each MAD-Handler application supporting MSCs, the MAD-Handler shall send a *Get MSC Table* command to each corresponding PSAM application that has successfully performed the *Start-up PSAM* command.

The response to the *Get MSC Table* command contains all PAN ranges supported by that PSAM application.

- 5.13.2.2 A The MAD-Handler shall store a record for each PAN range.

**NOTE:** Other implementations, e.g. relational data bases are allowed if the functionality defined here is obtained.

An example of an MSC Selection Record is given in Table 5.5.

Table 5.5 – MSC Selection Record (Example)

Data element	Value	Length
PAN <sub>FROM</sub>	PAN range from	4
PAN <sub>TO</sub>	PAN range to	4
ID <sub>PSAMAPP,N</sub>	TAPA application ID	1)
Pointer to the PSAM	Unique pointer to the PSAM supporting the ID <sub>PSAMAPP</sub> listed above	1)
DD	Discretionary Data	1)
<b>NOTES:</b>		
1) Implementation dependent.		

- 5.13.2.3 A Each MSC Selection Record record shall at least contain the PAN<sub>FROM</sub> and PAN<sub>TO</sub> data elements and a value that identifies both the PSAM Identification and ID<sub>PSAMAPP</sub>.

- 5.13.2.4 C Discretionary Data (DD) may be added to each MSC Selection Record as needed by the MAD-Handler.

**NOTE:** The prefix 4571xxxx used in the example above is indicated by the PSAM by setting PAN<sub>FROM</sub>=‘45710000’ and PSAM<sub>TO</sub>=‘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<sub>PSAMAPP</sub>) may be stored.

**NOTE:** More than one PSAM may support a given PAN range, e.g. if two PBS PSAMs are present for load sharing purposes in a terminal with several card readers.

- 5.13.2.5 A When storing entries from a given PSAM, the MAD-Handler 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.

- 5.13.2.6 C The MSC Selection Table should be kept in non-volatile memory to avoid the need for rebuilding it after power-up.



- 5.13.2.7 A The terminal shall, for each PSAM ID supported, retain up to 200 records in the MSC Selection Table.

**NOTE:** The total size may depend on other applications (and possible PSAMs) not defined by PBS.

### 5.13.3 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.

- 5.13.3.1 A For each MAD–Handler application supporting ICCs, the MAD–Handler shall send a *Get Supported AIDs* command to each corresponding PSAM application that has successfully performed the *Start–up PSAM* command.

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.

- 5.13.3.2 A The MAD–Handler shall store a record for each AID.

**NOTE:** Other implementations, e.g. relational data bases are allowed if the functionality defined here is obtained.

An example of contents in an AID Selection Record is given in Table 5.6.

Table 5.6 – AID Selection Record (Example)

Data element	Value	Length
LEN <sub>AID,N</sub>	Length of N'th AID	1
AID <sub>N</sub>	N'th AID	5 – 16
Card Name <sub>N</sub>	Default Card Name linked to the N'th AID	16
ASI <sub>N</sub>	Application Selection Indicator (N'th AID)	1
ID <sub>PSAMAPP,N</sub>	TAPA application ID	1)
Pointer to the PSAM	Unique pointer to the PSAM supporting the ID <sub>PSAMAPP</sub> listed above	1)
<b>NOTES:</b>		
1) Implementation dependent.		

- 5.13.3.3 A Each AID Selection Record shall at least contain:
- the AID (including length information)
  - ASI (Application Selection Indicator)

- a value that identifies both the PSAM Identification and the ID<sub>PSAMAPP</sub>.
- 5.13.3.4 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 issued for each AID in the AID Selection Table.
- NOTE:** If the MAD–Handler does not link the corresponding Card Names, the MAD–Handler may acquire the relevant Card Name “on the fly” during the application selection.
- 5.13.3.5 A For each AID received in the response to the *Get Supported AIDs* command, the MAD–Handler 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 for each AID in the AID Selection Table.
- When using the *Get Debit/Credit Properties* command for retrieving the ASI and/or Card Name, the Identifier shall be ‘0001’ 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 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’.
- 5.13.3.6 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 elements (PSAM Identification and ID<sub>PSAMAPP</sub> may be stored).
- NOTE:** More than one PSAM may support a given AID, e.g. if two PBS PSAMs are present for load sharing purposes in a terminal with several card readers.
- 5.13.3.7 A When storing entries from a given PSAM, the MAD–Handler 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.

- 5.13.3.8 C The AID Selection Table should be kept in non-volatile memory to avoid the need for rebuilding it at each power-up.
- 5.13.3.9 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 PBS.

#### 5.13.4 MSC Application Selection

When an MSC has been read, the MAD-Handler 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.

- 5.13.4.1 A The application selection mechanism for MSCs shall be based on the MSC Selection Table.
- 5.13.4.2 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.
- 5.13.4.3 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 MAD-Handler and PSAM applications pointed at from those records.
- 5.13.4.4 A If the MSC PAN is included in more MSC Selection Records with *different* PAN range widths, the MAD-Handler shall select the record with the smallest PAN range width (the most precisely defined prefix).
- 5.13.4.5 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”).

- 5.13.4.6 A Only the first 8 digits of the PAN shall decide whether the PSAM supports the actual PAN. Additional validations e.g. PAN length or modulus 10 check shall not be performed by the terminal.

#### **Searching an Unsorted MSC Selection Table**

The MAD-Handler 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 MAD-Handler 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.

### **5.13.5 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 MAD-Handler 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 MAD-Handler/PSAM application, e.g. the AIDs for “Dankort” and “Visa/Dankort”.

- 5.13.5.1 A ICC Application selection shall be performed according to ref. 36: “EMV, version 4.1”.

#### **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. 36: “EMV Version 4.1”.

- 5.13.5.2 B The terminal shall be able to handle a Candidate List containing at least 10 entries.
- 5.13.5.3 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.
- 5.13.5.4 A If an AID supported by the ICC matches an AID Selection Record, then the AID shall be included in the Candidate List.
- 5.13.5.5 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. 36: “EMV, version 4.1”, Application Note Bulletin no. 06, June 1st, 2002” for further details.

**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 9, “Data Elements”.

- 5.13.5.6 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. 36: “EMV, version 4.1” for these particular AIDs.

- 5.13.5.7 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.

- 5.13.5.8 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.

- 5.13.5.9 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:** The display of the Candidate List shall apply to requirement 5.13.5.13.

- 5.13.5.10 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.

**NOTE:** The display of the Candidate List shall conform to requirement 5.13.5.13.

- 5.13.5.11 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.

- 5.13.5.12 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.

**NOTE:** The display of the application shall apply to requirement 5.13.5.13.

### Display Rules

- 5.13.5.13 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.

- 5.13.5.14 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. 36: “EMV, version 4.1”.

**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 5.13.5.14 apply.

- 5.13.5.15 A If none of the AIDs supported by the ICC are supported by any of the PSAMs, the message code ‘12’ (“Use MAG Stripe”) shall be displayed on the Cardholder Display in order to initiate a MSC transaction.

### 5.13.6 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 5.14.

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:

- 5.13.6.1 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’.

- 5.13.6.2 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 5.14, where figure 5.3 “Fallback Handling (Combined Readers)” and figure 5.4 “Non-Fallback Handling (Combined Readers)” show the logical transaction flow.

- 5.13.6.3 C Combined MSC and ICC Application Selection shall be performed if:

- 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 shall be retained by issuing the *Get Debit/Credit Properties* command with the Identifier equal to ‘0002’.

5.13.6.4 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 5.13.5.

**NOTE:** The Card Name for the MSC shall be retained by issuing the *Get Debit/Credit Properties* command with the Identifier equal to ‘0002’.

5.13.6.5 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.

5.13.6.6 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.



## 5.14 Fallback from Chip (ICC) to Magnetic Stripe (MSC)

### 5.14.1 Introduction

In the present context the word “fallback” means the use of a particular technology when a preferred technology is not available for some reason.

This section defines the requirements for handling the fallback from ICC technology to magnetic stripe technology.

The general requirements defined by the major card schemes state that the use of the chip technology has first priority when handling cards provided with both a chip card and a magnetic stripe.

If the magnetic stripe is read first, the terminal will recognize that a chip is present through the value of the Service Code encoded on the magnetic stripe. The terminal must then ensure that the chip technology will be tried.

The Service Codes ‘2xx’ and ‘6xx’ indicate that a chip is present on the card, and an application corresponding to the magnetic stripe is present in the chip.

The validation of the Service Code will be performed by the PSAM. Based on the response from the PSAM, the terminal will recognize whether the chip technology shall be tried first or a fallback transaction may be initiated immediately.

The general requirements defined by the major card schemes also state that fallback transactions must be online processed. Finally, general requirements state that fallback transactions may not be accepted in all environment.

The requirements for online processing or rejection in specific environments (e.g. Cardholder Activated Terminals) will be handled by the PSAM.

### 5.14.2 General Requirements

Since the reading of card data (either from the chip or the magnetic stripe) is performed by the terminal, and since the application selection is also performed by the terminal (MAD-Handler), a number of requirements are defined for the handling of fallback from chip to magnetic stripe.

- 5.14.2.1 A If the card has a chip i.e. Service Code ‘2xx’ or ‘6xx’, the terminal shall always try to perform the transaction with the chip technology first.

- 5.14.2.2 A In case of a terminal with separate readers, it may happen that the card is swiped/inserted in the magnetic stripe reader first. In that case the terminal shall inform the merchant and cardholder that the chip reader shall be tried first if Service Code ‘2xx’ or ‘6xx’.
- NOTE:** The response to *Initiate MSC Payment* command will indicate whether the Service Code on the magnetic stripe indicates that an ICC is present on the card.
- 5.14.2.3 A If any of the Debit/Credit applications supported by both the ICC and the terminal are blocked, then fallback to magnetic stripe shall not be initiated.
- 5.14.2.4 A If the transaction is aborted due to wrong manipulation (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.
- 5.14.2.5 A Fallback is not allowed from a non-Debit/Credit application, like a loyalty application, to the Debit/Credit application on the magnetic stripe.
- 5.14.2.6 A If the transaction is cancelled before completion, either by the merchant or the cardholder, chip technology keeps priority and fallback to magnetic stripe shall not be initiated.

The figures 5.1 and 5.2 show the procedures for handling of fallback from ICC technology to magnetic stripe technology for separate readers.

The figures 5.2 and 5.3 show the procedures for handling of fallback from ICC technology to magnetic stripe technology for a combined reader with “MSC read before ICC”.

Figures 5.3 and 5.5 show the procedures for handling of fallback from ICC technology to magnetic stripe technology for a combined reader with ‘ICC read before MSC’

More information concerning the different types of combined readers are described in section 5.13.6.

Figure 5.4 shows the handling of cards where the Service Code is different from ‘2xx’ or ‘6xx’ for combined readers. Note that fallback in these cases are not allowed.

**NOTE:** Please note that the figures 5.1 to 5.5 describes functional requirements. Other implementations (e.g. where checks are made in a different order) may fulfill the requirements mandated in this specification. If PSE is supported, additional handling may be necessary (command etc.) to e.g. check whether blocked applications exists in the card or not.

Terminals with combined readers may automatically initiate fallback to magnetic stripe, while terminals with separate read-

ers shall be able to guide the merchant and/or the cardholder to use either of the readers in case of fallback situations.

In figure 5.1 a flag called ‘ICC Reader Tried’ has been introduced. This flag shall handle the situations when a card with chip has been swiped/inserted in a separate magnetic stripe reader without previous attempt to use the (separate) chip reader.

Since the PSAM is the component validating the Service Code from the magnetic stripe, the terminal shall first try to initiate a ‘normal’ magnetic stripe transaction before a the fallback transaction. The response from PSAM for initiate of the ‘normal’ magnetic stripe transaction will indicate if a chip is present and must be tried first.

5.14.2.7 A The terminal shall indicate the difference between a ‘normal’ magnetic stripe transaction and a fallback transaction by setting the value for POS Entry Mode, position 3 to ‘7’.

5.14.2.8 A When separate readers are utilized, the merchant shall confirm (physically) that the card is inserted correct and initiating of fallback is accepted.

**NOTE:** An example of the message displayed at the Merchant Display could be: “Card inserted correctly?” / “Kort isat korrekt?”.

5.14.2.9 B When 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 magstripe?” / “Fortsæt med magnetstripe?”.

5.14.2.10 A When a combined reader is utilized, the terminal shall issue a *Get Debit/Credit Properties* command with the “Identifier” equal to ‘0002’ (indicating additional MSC information) and the track 2 data as input parameter.

The PSAM will respond with Card Name, Card Service Info and Service Code. The Service Code is used by the terminal to decide whether the fallback procedure is applicable or not.

More information concerning the handling of cards where the magnetic stripe is not a back-up for an application in the ICC are described in section 5.13.6.

### 5.14.3 The role of the PSAM

After the *Initiate EMV Payment* command has been issued, it is the task of the PSAM together with the host systems to verify that the conditions for allowing fallback are met.

Examples of conditions to fulfil before initiating fallback are:

- Service Code must indicate “ICC to be used” (‘2xx’ or ‘6xx’).
- The transaction has failed (resulting in an Authorization Advice / Reversal Advice)
- Neither a TC nor an AAC has been received from the card.
- The cardholder or the merchant has not deliberately cancelled the transaction (e.g. by activating a button).
- The Application Status Words (ASW1–ASW2) are *not* in the range:
  - ‘0000’ ≤ ASW1–ASW2 < ‘1100’
  - ‘1A00’ ≤ ASW1–ASW2 ≤ ‘2000’

**NOTE:** The PSAM related conditions for allowing fallback are subject to changes and may be changed without further notice. Changes will have no impact on the terminal handling of fallback.

- 5.14.3.1 A The terminal shall not decide whether fallback is approved or not. It is handled solely by the PSAM/host system.

#### 5.14.4 Final Decision

The ASW1–ASW2 codes given in the responses from the PSAM will inform the terminal about the actual status.

- 5.14.4.1 A If the response to the *Initiate MSC Payment* command indicates ASW1–ASW2 = ‘1222’ (Service Code; ICC to be used), then the terminal shall initiate a fallback transaction if the ICC reader has already been tried.
- 5.14.4.2 A If none of the requirements in section 5.14.2 prohibit fallback and the response to the *Complete Payment* command indicates ASW1–ASW2 in the range ‘10FB’ – ‘10FD’, then the terminal shall initiate fallback.

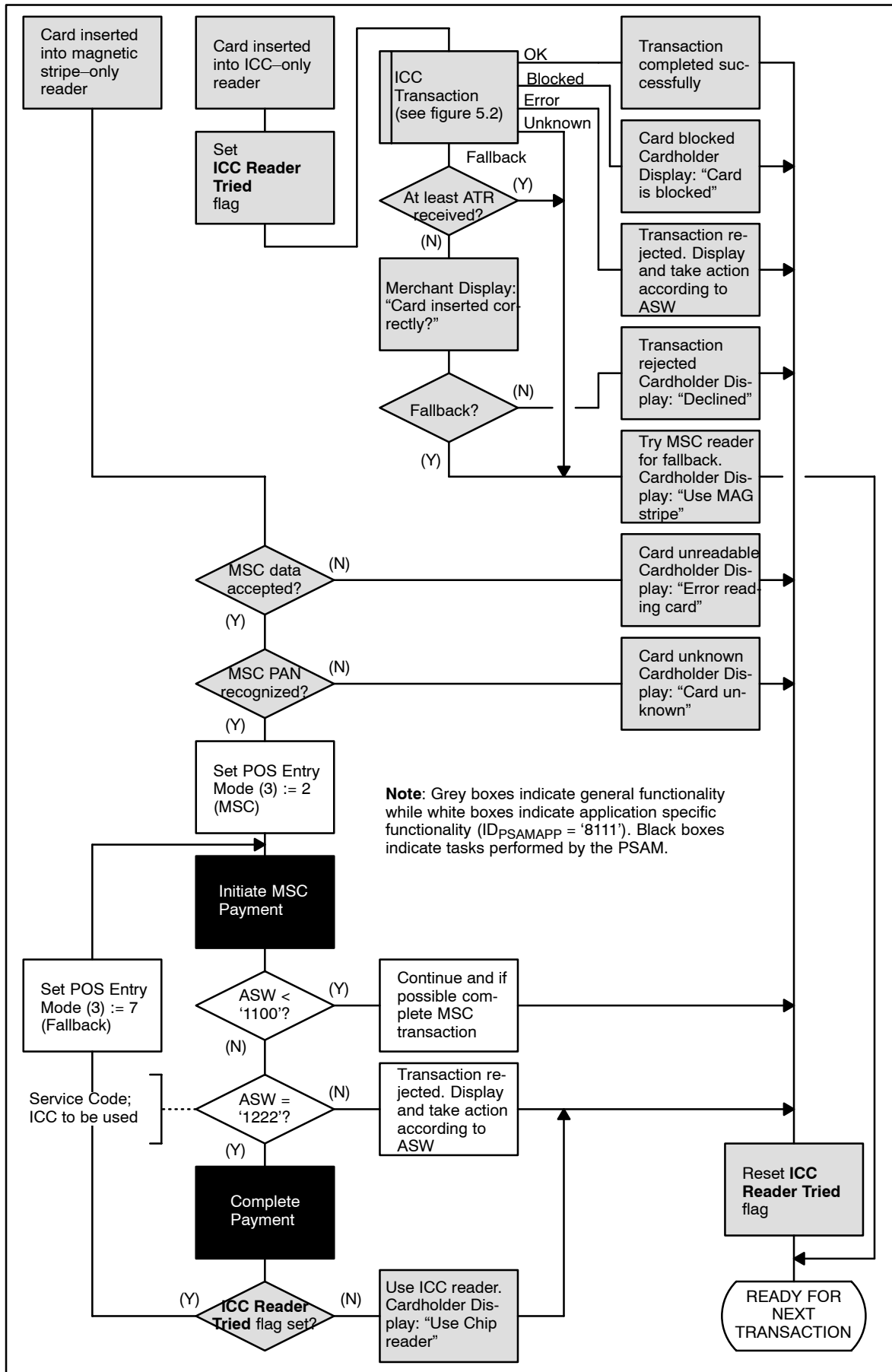


Figure 5.1 – Fallback Handling (Separate Readers)

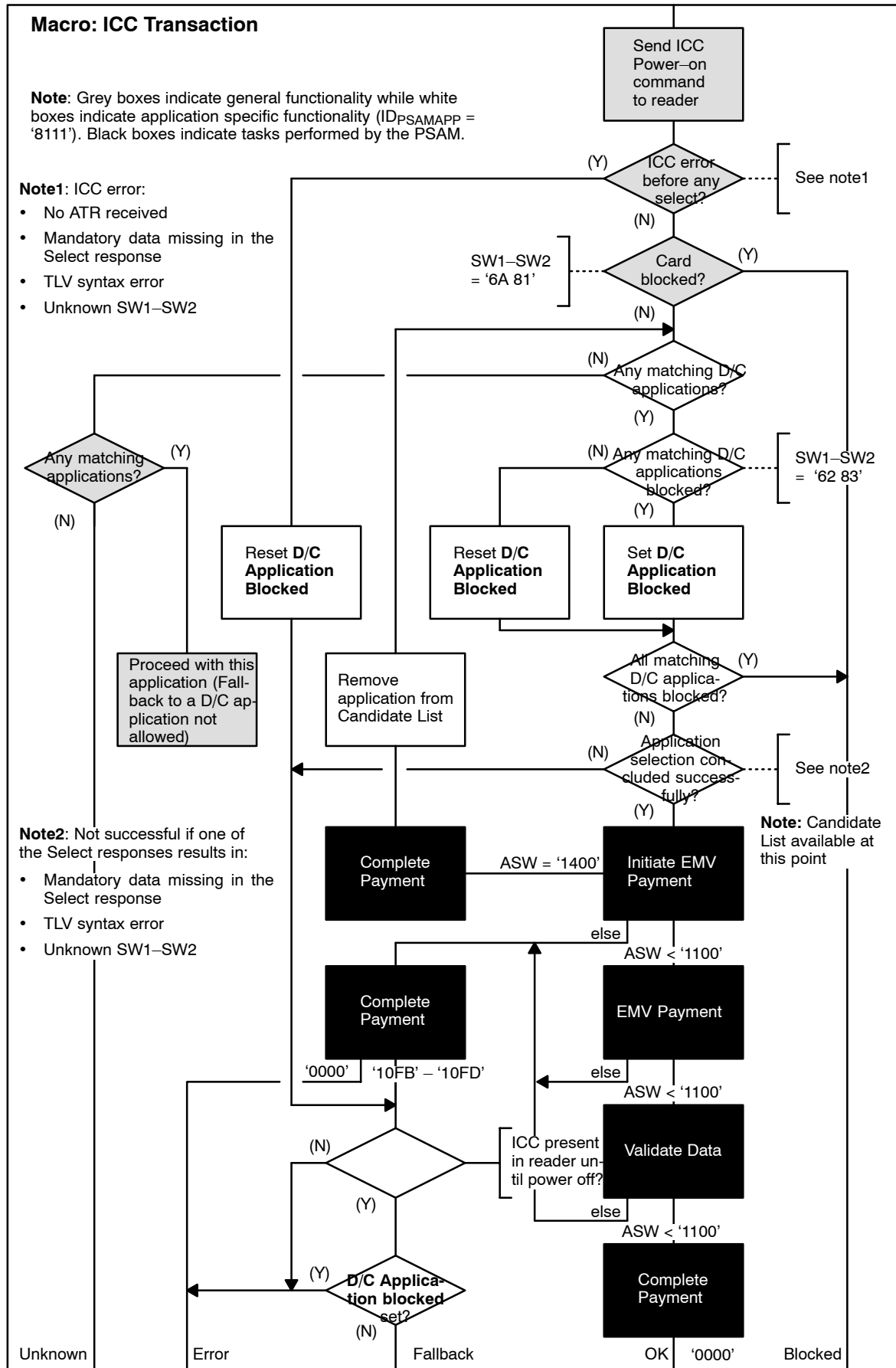


Figure 5.2 – Fallback Handling – ICC Transaction

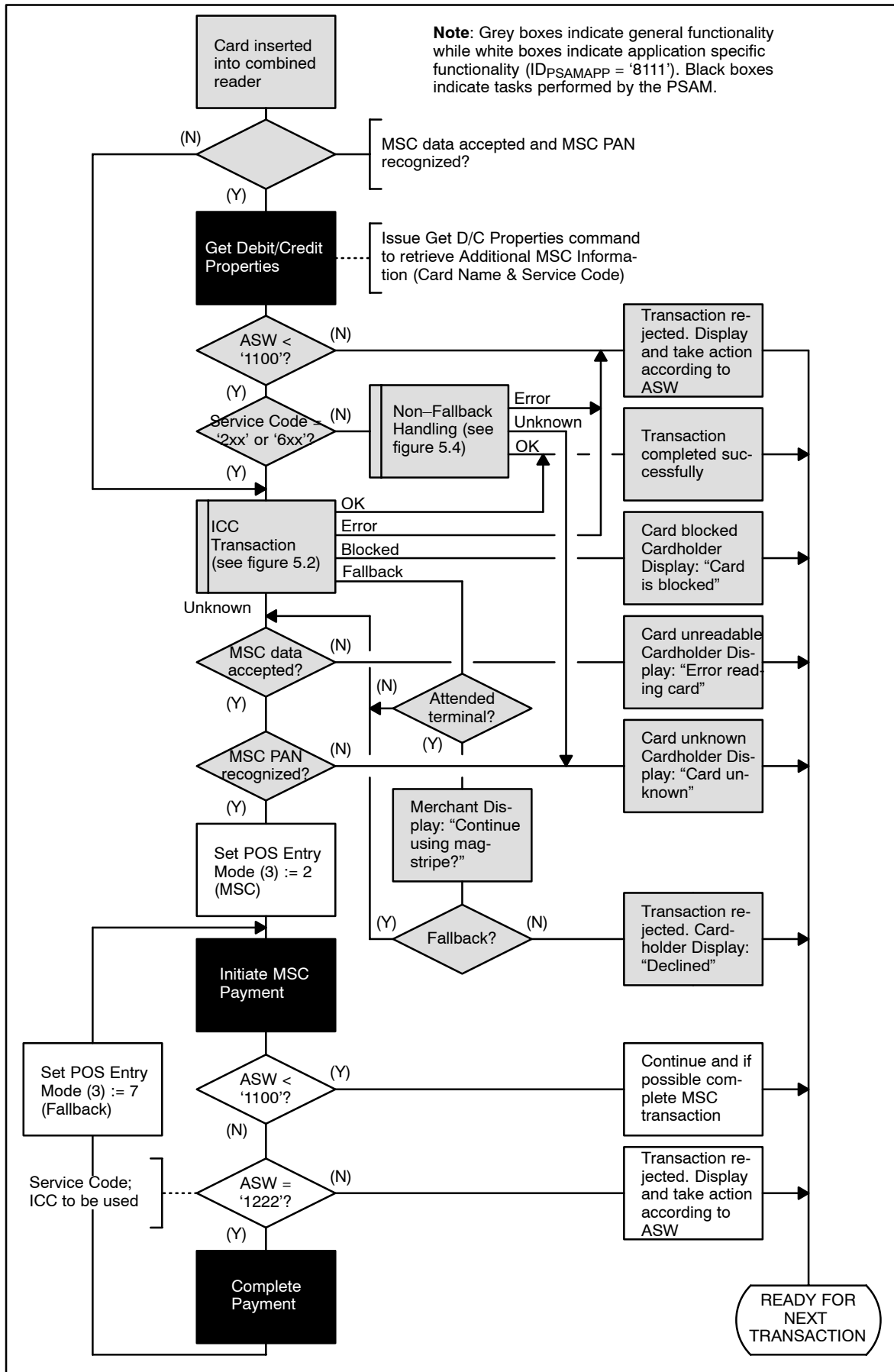


Figure 5.3 – Fallback Handling (Combined Readers) – MSC read before ICC

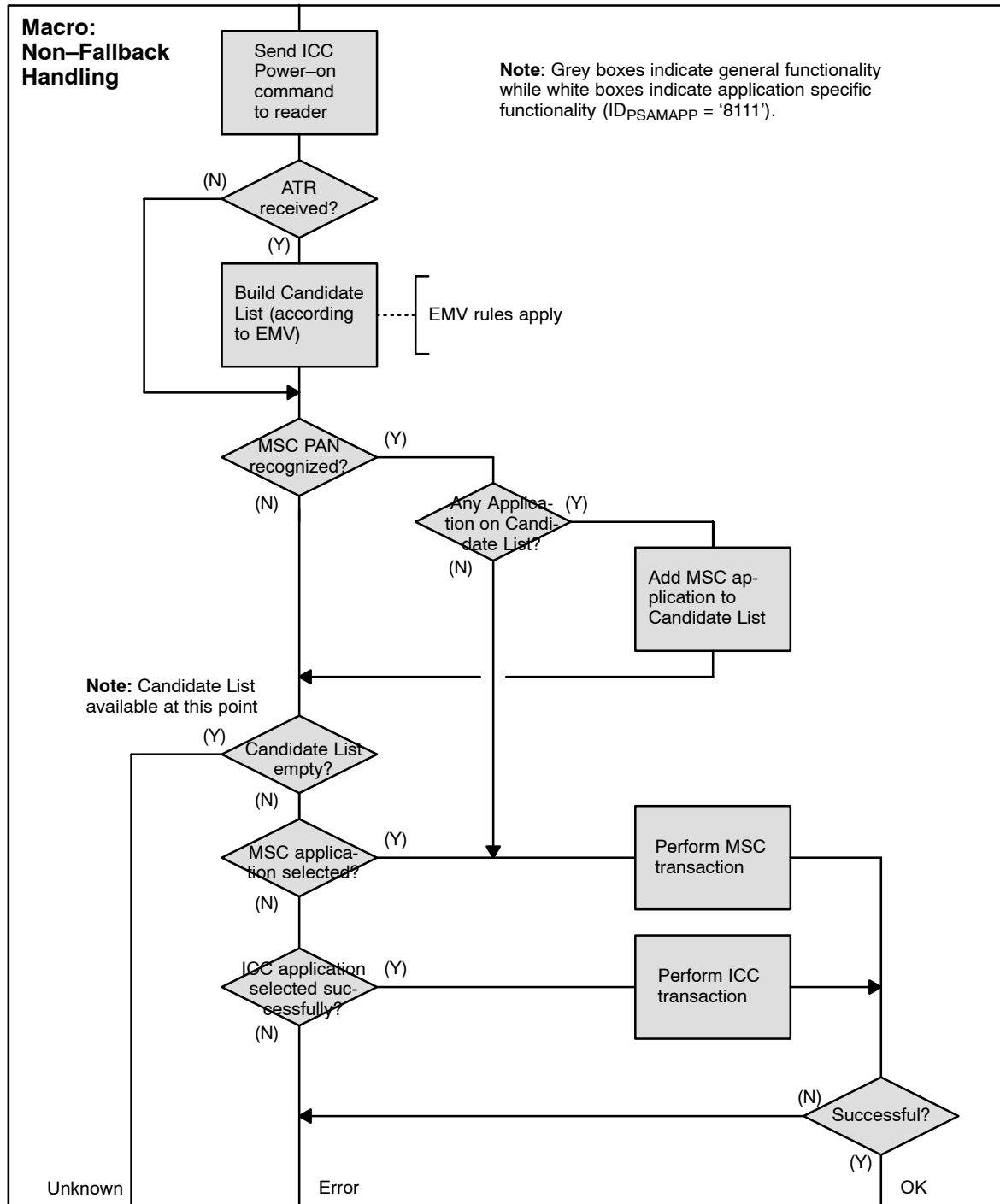


Figure 5.4 – Non-Fallback Handling (Combined Readers)



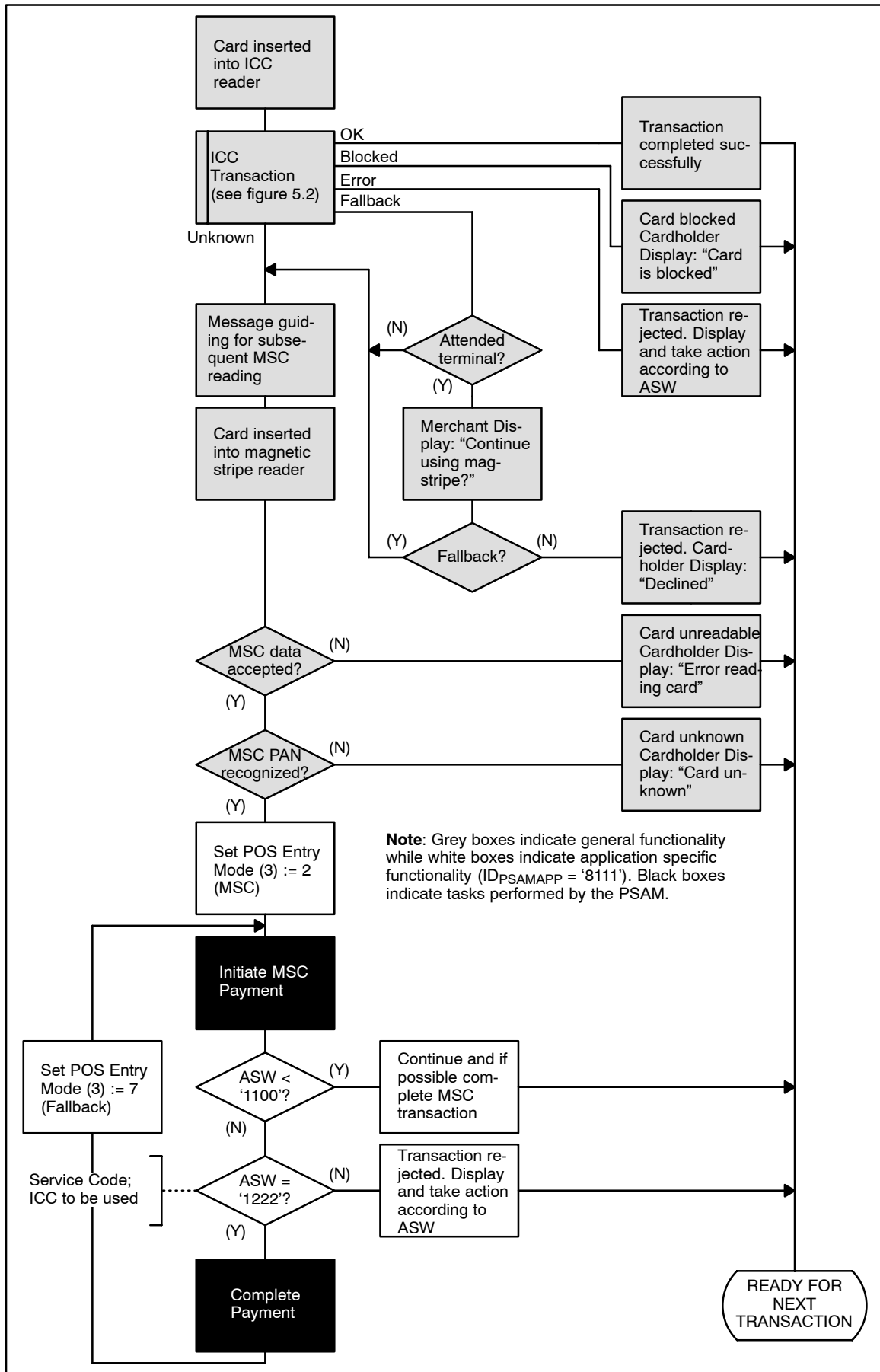


Figure 5.5 – Fallback Handling (Combined Readers) – ICC read before MSC

## 5.15 Language Selection

### 5.15.1 General Requirements

The terminal may be able to support more than one language for the text on the Cardholder Display, as defined in section 5.6.4, “Sub-handler, Cardholder Display”.

5.15.1.1 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.

5.15.1.2 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.

5.15.1.3 B When a transaction is completed and the terminal returns to idle state (ready to service a new cardholder), the default language (i.e. Danish) shall be selected automatically.

5.15.1.4 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. Danish).

**NOTE:** The Time-out value may depend on the environment in which the terminal is used.

### 5.15.2 ICC Language Selection

The ICC may include the data element Language Preference (tag ‘5F2D’).

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.

5.15.2.1 A The ICC Language Selection shall be performed according to ref. 36: “EMV, version 4.1”.

5.15.2.2 A Language selection based on the data element Language Preference shall be performed before the *Initiate EMV Payment* command is initiated.

5.15.2.3 B Language selection based on the data element Language Preference shall overrule a language selection performed previously and manually.

5.15.2.4 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.

- 5.15.2.5 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.

This page is intentionally left blank

## 6. Debit/Credit Functionality

### 6.1 Application Initialization

#### 6.1.1 Introduction

- 6.1.1.1 A After the CAD is powered on, communication between the CAD and the PSAM shall be established according to the description in ref. 40: “TAPA, Application Architecture Specification”.
- 6.1.1.2 A Initialization of the debit/credit application shall be established as defined in figure 6.1 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.

6.1.1.3 A If more PSAMs are present for handling debit/credit transactions, initialization shall be performed for each of these PSAMs.

6.1.1.4 A The ID<sub>PSAMAPP</sub> 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.

## 6.1.2 Power On

6.1.2.1 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.

6.1.2.2 A This step shall not be performed if the PSAM has already been powered on to initialize another application.

6.1.2.3 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.

6.1.2.4 A The following data elements:

- Type of application (“PBS Debit/Credit”)
- PSAM ID
- MAD-Handler ID
- Terminal Software version no. (Build date)
- EMV Checksum
- PSAM Code Checksum
- PSAM Config Checksum

shall be available on paper e.g. printed in a terminal report.

6.1.2.5 C The data elements listed in requirement 6.1.2.4 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’.

6.1.2.6 B The following data elements (in addition to the data elements listed in requirement 6.1.2.4):

- PED info
- PSAM version
- PSAM Subversion
- Service Packs requested
- Host Interface info (e.g. IP-address, Port no., communication network)

shall be available on paper e.g. printed in a terminal report.

- 6.1.2.7      C      The data elements listed in requirement 6.1.2.6 may be displayed after power-up on the Merchant Display (attended terminal) or the Cardholder Display (unattended terminal).

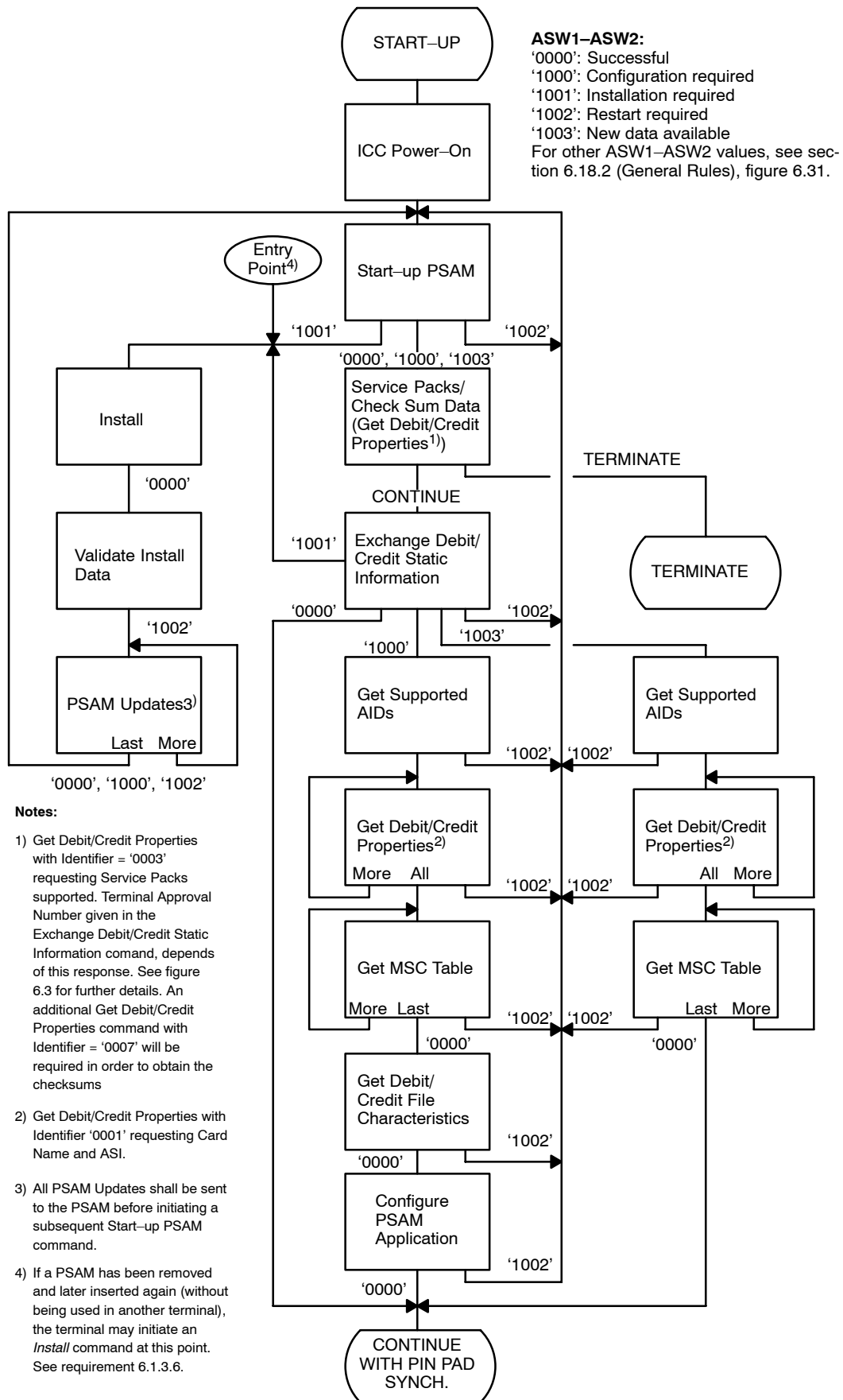


Figure 6.1 – Initialization Sequence – Normal Flow



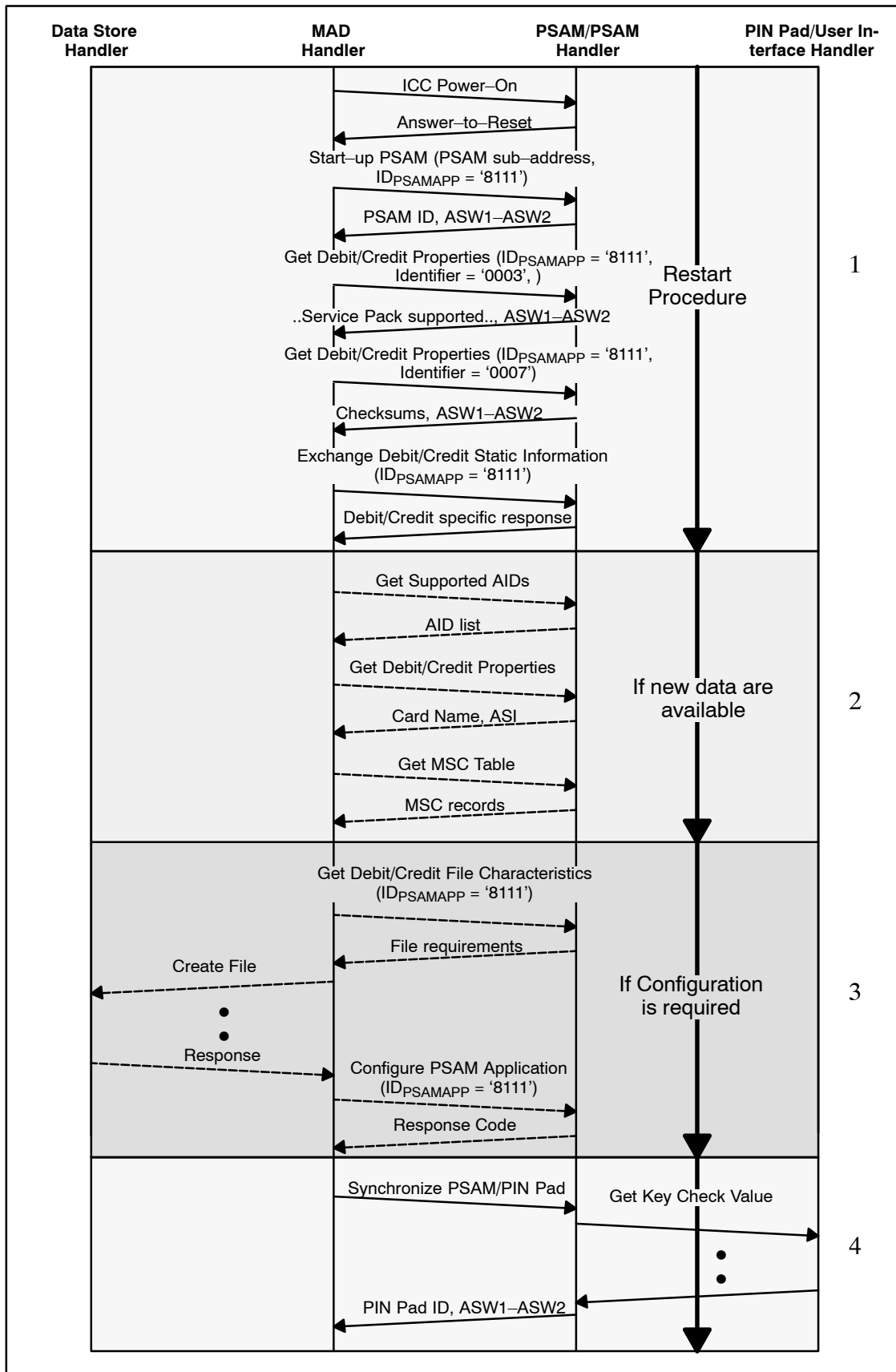


Figure 6.2 – PSAM Debit/Credit Application Initialization Sequence (without Installation)

### 6.1.3 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)
- *Exchange Debit/Credit Static Information*

#### Start-up PSAM

- 6.1.3.1 A The MAD-Handler shall send the *Start-up PSAM* command to the PSAM after receiving the ATR. The command shall contain the sub-address assigned to the reader in which the PSAM is inserted.
- 6.1.3.2 A The MAD-Handler shall retain the PSAM Identification returned by the PSAM along with the assigned sub-address.
- 6.1.3.3 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')
- 6.1.3.4 A If ASW1-ASW2 has the value '0000' (Successful), reading of PSAM data is optional and file configuration shall *not* be performed.
- NOTE:** 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.
- 6.1.3.5 A If ASW1-ASW2 has the value '1000' (Configuration required), reading PSAM data *and* performing file configuration are mandatory.
- 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.
- 6.1.3.6 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 termi-

nal), 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 substituted, an Installation transaction may be relevant or desirable.

- 6.1.3.7 A If ASW1–ASW2 has the value ‘1002’ (Restart required), the *Start–up PSAM* command shall be resend.
- 6.1.3.8 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 11 (Service Packs)

- 6.1.3.9 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.
- 6.1.3.10 A The MAD–Handler shall choose the highest mutual supported Service Pack No. This number shall be indicated in Terminal Approval Number send in the succeeding *Exchange Debit/Credit Static Information* command.

**NOTE:** How to select the the highest mutual supported Service Pack No. is explained in figure 6.3.

- 6.1.3.11 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 mutually supported.

**NOTE:** The PSAM will always support baseline.

- 6.1.3.12 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.

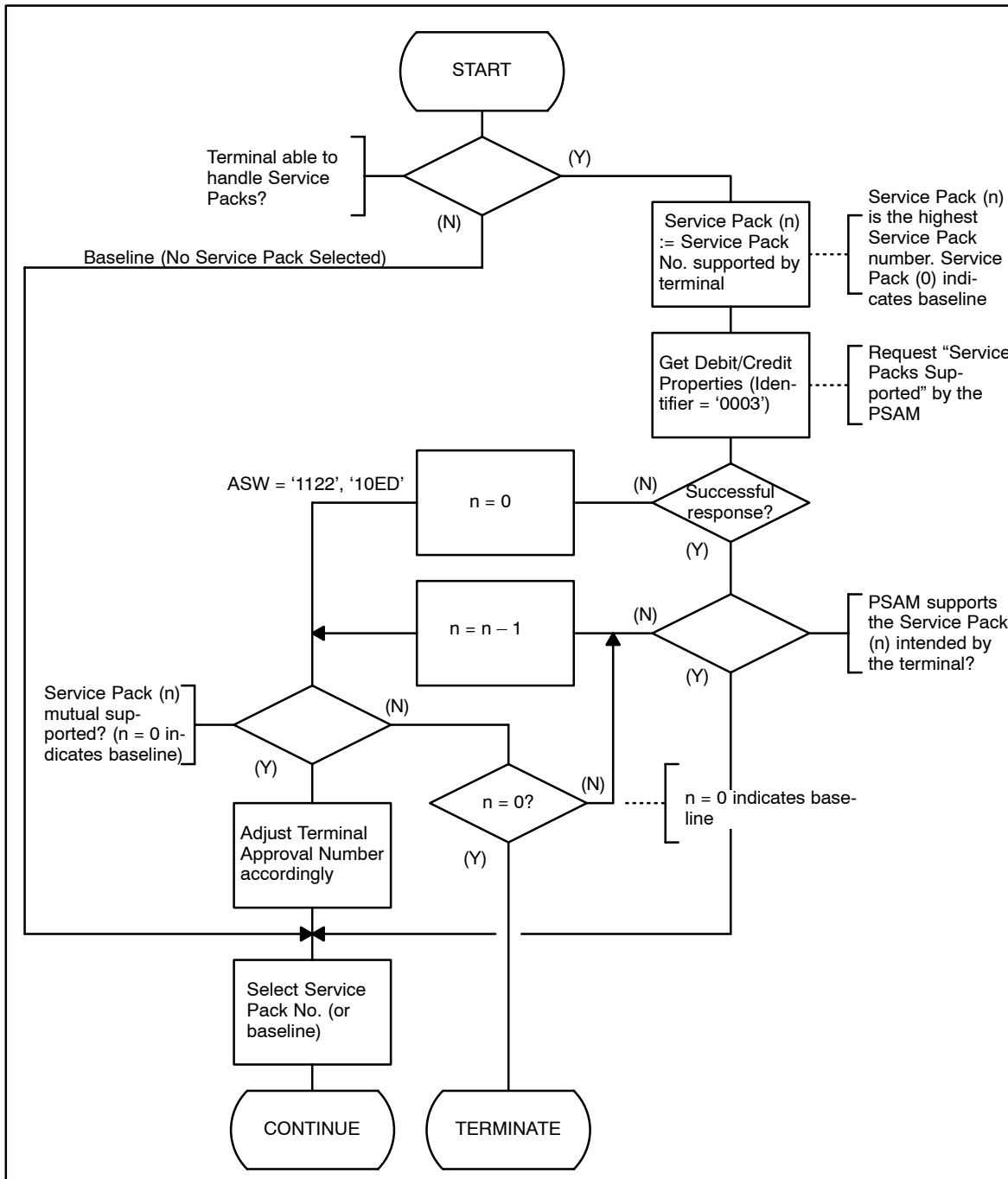


Figure 6.3 – Service Pack Check

- 6.1.3.13 A The Terminal Approval No. (3 MSB) shall be adjusted according to the Service Pack selected.

**Exchange Debit/Credit Static Information**

- 6.1.3.14 A The MAD-Handler shall send the *Exchange Debit/Credit Static Information* command to the PSAM.
- 6.1.3.15 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.

- 6.1.3.16 A The terminal shall contain one merchant table with the contents given in table 6.1. The merchant table is used when printing.

Table 6.1 – Terminal Merchant Table

Data element	Value	Length
ME No.	Merchant number	5
ME <sub>NAME</sub>	Merchant name	18
ME <sub>CITY</sub>	Merchant city	16
ME <sub>ADDRESS</sub>	Merchant address	24
ME <sub>ZIP</sub>	Merchant zip code	8
ME <sub>PHONE</sub>	Merchant Phone No.	24
ME <sub>BRN</sub>	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”.

- 6.1.3.17 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 Information. 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.

- 6.1.3.18 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.
- 6.1.3.19 A The MAD-Handler shall indicate whether the *Confirm Amount* command is requested for Original Authorizations or not. This is indicated in “Info Level” in the *Exchange Debit/Credit Static Information* command.

### 6.1.4 Installation

An Installation sequence requires these steps in the listed order:

- *Install*
- Installation Request (host message)
- *Validate Install Data*
- PSAM Update sequence (host messages)
- *PSAM Update*

The requirements concerning the Installation Transaction is listed in section 6.16.2 (Installation Transaction).

The requirements concerning the PSAM Updates is listed in section 6.16.7 (PSAM Update Transaction).

- 6.1.4.1 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.

### 6.1.5 New Application Data

- 6.1.5.1 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*
- *Get MSC 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 the Card Names and ASIs (Application Selection Indicator) 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.

- 6.1.5.2      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. 40: “TAPA, Application Architecture Specification”.

## 6.1.6 Configuration

- 6.1.6.1      A      If configuration is required (indicated in the response to the *Exchange Debit/Credit Static Information* command), the following commands shall be performed after the last *Get MSC Table* command:

- *Get Debit/Credit File Characteristics*
- *Create File*
- *Configure PSAM Application*

The *Get Debit/Credit File Characteristics* command is used by the terminal to retrieve the file usage information from the PSAM application, 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 indicated 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.

## 6.1.7 PSAM/PIN Pad Synchronization

As the last step in the initialization sequence, the synchronization between the PSAM and PIN Pad(s) is performed.

- 6.1.7.1 A The following command shall be performed as the last command in the initialization sequence:
- *Synchronize PSAM/PIN Pad*
- 6.1.7.2 A The secure zone between the PBS PSAM and the PIN Pad shall be established according to ref. 40: “TAPA, Application Architecture Specification”. For further details, see figure 6.4.
- 6.1.7.3 A The terminal shall perform a synchronization of each PIN Pad attached.
- 6.1.7.4 A The synchronization sequence shall be initiated by the terminal even though the terminal does not have a PIN Pad.
- 6.1.7.5 A If no PIN Pad is present, the Response Code shall be ‘FFFB’ (Unsupported operation) in the response to *Get Key Check Value* command.
- 6.1.7.6 C If the secure zone cannot be established, the terminal may perform signature and No CVM based transactions only.

The synchronization sequence depicted in figure 6.4 will also be initiated by the PSAM each time an *Initialize Payment* command (requiring PIN) is issued as well.



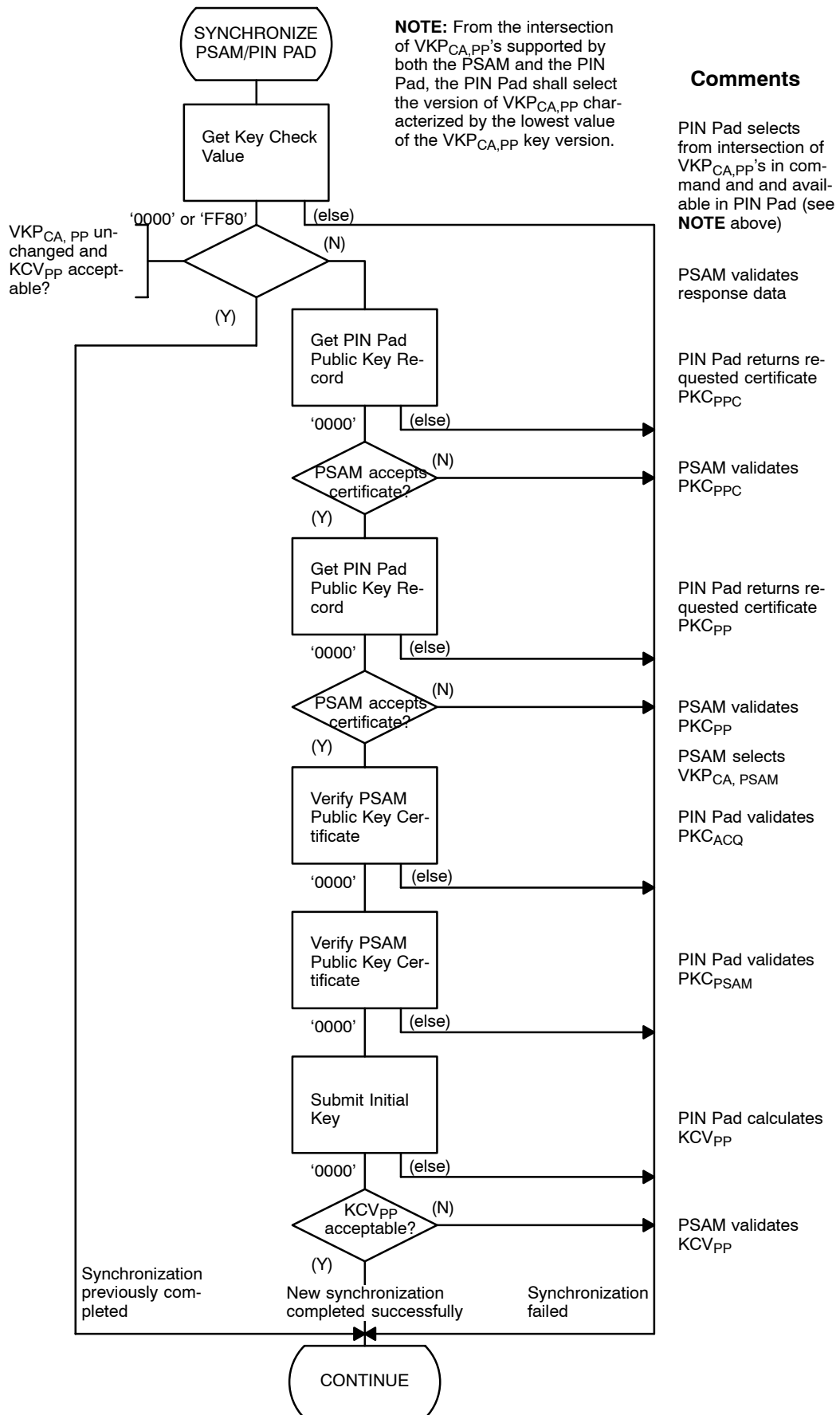


Figure 6.4 – PSAM/PIN Pad Synchronization Sequence

## 6.1.8 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 withdrawal power from the PSAM.

**NOTE:** Each PSAM application requires an individual *PSAM Shutdown* command.

- 6.1.8.1      A      The *PSAM Shutdown* command shall conform to the format defined in ref. 40: “TAPA, Application Architecture Specification”.

## 6.2 Business Calls

Business Call is the term used for the functions initiated by the Merchant Application, requesting the type of transaction or process to be initiated.

The following Business Calls are defined:

Card related Business Calls:

- Purchase
- Original Authorization
- Supplementary Authorization
- Capture
- Reversal (Authorization)
- Refund

Administrative Business Calls:

- Installation
- Advice Transfer
- PSAM Update
- PSAM Deactivation

Examples of possible transactions related to card related Business Calls can be found in table 6.2 to table 6.7.

### 6.2.1 Purchase

Purchase is used when the amount to be paid is known (Accurate Amount) and a financial message shall be generated.

The Purchase may result in either:

- an online Financial Request or
- an offline 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.

Table 6.2 – Transactions initiated by the Purchase call

Purchase															
Amount	Accurate Amount														
Card Data	MSC					ICC					Key entered				
Card present	Yes					Yes					Yes		No		
CVM	PIN	Signature		No CVM		PIN	Signature		No CVM		Signature		No CVM		
<b>Validation:</b>															
Processing	On	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off
Cryptogram						ARQC		ARQC		ARQC					
<b>Output:</b>															
Auth.Msg.	–	–	–	–	–	AR	–	AR	–	AR	–	–	–	–	–
Fin. Msg.	FR	FR	FA	FR	FA	FA	FA	FA	FA	FA	FA	FR	FA	FR	FA
Cryptogram						TC	TC	TC	TC	TC	TC				
<b>Environments:</b>															
Retail	X	X	(X)			X	X	X	X			(X)	(X)		
Mail order														X	(X)
CAT	X			X	(X)	X	X				X	X			
Restaurant (gratuity)															
Car Rental															
Hotel															
Fuel dispenser															

**Legend:** On = Online Authorization, Off = Offline Authorization, AR = Authorization Request, FR = Financial Request, FA = Financial Advice, X = applicable, (X) = Fallback, ARQC = Authorization Request Cryptogram, TC = Transaction Certificate.

## 6.2.2 Original Authorization

Original Authorization is used when the exact amount is not known when the process of paying with the card is initiated (Estimated Amount). Alternatively, if the Authorization/Capture is not performed at the same terminal/time. The Original Authorization will initiate the process for authorization, either online or offline, but no financial message will be generated. If the Original Authorization is completed successfully, then a Token is generated.

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

The Token is stored in the Merchant Application.

The estimation of the amount may dependent of 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.

Table 6.3 – Transactions initiated by the Original Authorization call

Original Authorization																	
Amount	Estimated Amount																
Card Data	MSC					ICC						Key entered					
Card present	Yes					Yes						Yes			No		
CVM	PIN	Signature		No CVM		PIN	Signature		No CVM		Signature	No CVM		No CVM			
<b>Validation:</b>																	
Processing	On	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off
Cryptogram						ARQC		ARQC		ARQC							
<b>Output:</b>																	
Message	AR	AR	AA	AR	AA	AR	AA	AR	AA	AR	AA	AR	–	AR	–	AR	–
Token	X	X	X	X	X	X	X	X	X	X	X	X		X		X	
Cryptogram						TC	TC	TC	TC	TC	TC						
<b>Environments:</b>																	
Retail																	
Mail order																	X
CAT																	
Restaurant (gratuity)				X		X	(X)			X	(X)			(X)			
Car Rental				X		X	(X)			X	(X)			(X)			(X)
Hotel				X		X	(X)			X	(X)			(X)			(X)
Fuel dispenser	X			X		X	(X)			X	(X)						

**Legend:** On = Online Authorization, Off = Offline Authorization, AR = Authorization Request, AA = Authorization Advice, X = applicable, (X) = Fallback.

### 6.2.3 Supplementary Authorization

Supplementary Authorization is used when the Original Authorization has already been completed, but the amount has been re-estimated and the new value is higher than the amount already authorized. The amount specified in an Supplementary Authorization shall be the difference between the new estimated amount and the amount already authorized.

One or more Supplementary Authorizations may follow an Original Authorization.

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.

Table 6.4 – Transactions initiated by the Supplementary Authorization call

	Supplementary Authorization		
Amount	Estimated Amount		
Card Data	Token		
Card Data (original)	MSC	ICC	Key entered
Card present	No	No	No
CVM	No CVM	No CVM	No CVM
<b>Validation:</b>			
Processing	On	On	On
Cryptogram			
<b>Output:</b>			
Auth. Msg.	AR	AR	AR
Token	X	X	X
Cryptogram		TC <sup>1)</sup>	
<b>Environments:</b>			
Retail			
Mail order			
CAT			
Restaurant (gratuity)	X	X	X
Car Rental	X	X	X
Hotel	X	X	X
Fuel dispenser			
<b>Legend:</b> On = Online validation, AR = Authorization Request, TC = Transaction Certificate (Initial TC from Token), X = applicable, (X) = Fallback, <sup>1)</sup> = part of the Token.			

## 6.2.4 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 (and zero or more 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 presence of a card is not required.

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.

Table 6.5 – Transactions initiated by the Capture call

	Capture					
Amount	Accurate Amount					
Card Data	Token					
Card Data (original)	MSC		IOC		Key entered	
Card present	No		No		No	
CVM	Signature	No CVM	Signature	No CVM	Signature	No CVM
<b>Validation:</b>						
Processing	Off	Off	Off	Off	Off	Off
Cryptogram						
<b>Output:</b>						
Fin. Msg.	FA	FA	FA	FA	FA	FA
Cryptogram			TC	TC		
<b>Environments:</b>						
Retail						
Mail order						X
CAT						
Restaurant (gratuity)	X		X	X	X	
Car Rental	X		X	X	X	X
Hotel	X		X	X	X	X
Fuel dispenser		X		X		
<b>Legend:</b> Off = Offline validation, FA = Financial Advice, TC = Transaction Certificate (Initial TC from Token, based on estimated amount), X = applicable, (X) = Fallback.						

## 6.2.5 Reversal (Authorization)

Reversal (Authorization) is used when an authorization has been completed, but no Capture is going to be initiated due to cancellation of the payment process.

Table 6.6 – Transactions initiated by the Reversal (Authorization) call

	Reversal (Authorization)		
Amount	Accurate Amount		
Card Data	Token		
Card Data original	MSC	ICC	Key entered
Card present	No	No	No
CVM	–	–	–
<b>Validation:</b>			
Processing	Off	Off	Off
Cryptogram			
<b>Output:</b>			
Fin. Msg.	RA	RA	RA
Cryptogram			
<b>Environments:</b>			
Retail			
Mail order			X
CAT			
Restaurant (gratuity)	X	X	X
Car Rental	X	X	X
Hotel	X	X	X
Fuel dispenser	X	X	X
<b>Legend:</b> Online Reversal, Off = Offline Reversal, RA = Reversal Advice, X = applicable, (X) = Fallback.			

## 6.2.6 Refund

Refund is used when a “reverse” Purchase shall be completed.

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.

- 6.2.6.1 A No Cashback amount shall be specified for Refund transactions.

Table 6.7 – Transactions initiated by the Refund call

	Refund					
Amount	Accurate Amount					
Card Data	MSC		ICC		Key entered	
Card present	Yes		Yes		Yes	
CVM	Signature		Signature		Signature	
<b>Validation:</b>						
Processing	On	Off	On	Off	On	Off
Cryptogram						
<b>Output:</b>						
Auth. Msg.	–	–	–	–	–	–
Fin. Msg.	FR	FA	FR	FA	FR	FA
Cryptogram						
<b>Environments:</b>						
Retail	X	(X)	X	X	(X)	(X)
Mail order						
CAT						
Restaurant (gratuity)						
Car Rental						
Hotel						
Fuel dispenser						
<b>Legend:</b> On = Online Authorization, Off = Offline Authorization, AR = Authorization Request, FR = Financial Request, FA = Financial Advice, X = applicable, (X) = Fallback.						

## 6.2.7 Business Calls and Terminal Environments

The defined Business Calls may not be relevant in all terminal environments.

- |         |   |  |
|---------|---|--|
| 6.2.7.1 | A | If the cardholder shall be able to pay for goods, services or cash, then the terminal shall support Purchase and/or Capture. |
| 6.2.7.2 | B | If the terminal is attended and either Purchase or Capture is supported, then the terminal shall support Refund as well.     |
| 6.2.7.3 | A | If Capture is supported, then Original Authorization and Reversal (Authorization) shall be supported as well.                |
| 6.2.7.4 | C | If Capture is supported, then Supplementary Authorization may be supported.  |

## 6.3 Gratuity and other surcharges

The Business Calls can further be categorized into transactions where the amount is known when the transactions is initiated (“Amount accurate”) and transactions where the amount is *not* known when the transaction is initiated (“Amount estimated”). Table 6.8 gives an overview of the Business Calls and the related amounts.



Table 6.8 – Business Calls Vs. Amount

Business Call	Amount	
	Accurate	Estimated
Purchase	○	
Refund	○	
Original Authorization		○
Supplementary Authorization		○
Capture	○	
Reversal (Authorization)		○

### 6.3.1 Purchase & Refund

As mentioned in the 6.8, the transaction amount shall be known whenever a Purchase or Refund transaction is initiated or at least known during the first transaction steps.

- 6.3.1.1 A No surcharging or fees shall be added to the transaction amount after the transaction (Purchase or Refund) is initiated and the amount is transferred to the PSAM.

**NOTE:** Gratuity and surcharge may be added in the response to the *Get Amount 2/Get Amount 3* command. In case of a Single Unit Terminal, any dialogue with the merchant shall be completed before PIN entry is initiated.

If the transaction is PIN based, the transaction amount (amount accurate) will appear on the Cardholder Display when entering the PIN, as well as printed on the receipt.

For a signature based transaction, the transaction amount (amount accurate) will appear on the receipt that the cardholder signs (or the merchant in case of a Refund transaction).

### 6.3.2 Token Based Transactions

Token based transactions are implemented in order to allow payment situations where the exact transaction amount is *not* known when the transaction is initialized.

Table 6.9 shows the 4 types of Token based transactions.

Table 6.9 – Transaction Request Vs. Transaction Data

Transaction Request	Transaction Data	
	Input	Output
Original Authorization	Card read <sup>1</sup> / Key entered	Token
Supplementary Authorization	Token	Token

Capture	Token	Financial Advice
Reversal (Authorization)	Token	Reversal Advice
<b>Legend:</b> <sup>1)</sup> Card read covers both EMV & MSC.		

Token based transactions are intended to handle the following payment situations (examples):

- Fuel dispensers where an Original Authorization is performed before refueling may begin. A Capture will (automatically) be performed when the tanking is finished and the exact amount is known.
- Restaurants and similar environments where the cardholder choose to pay an extra fee, typically gratuity. When the transaction is initiated, an Original 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 initiate an Original Authorization during the check-in or the start of the lease. If it, during the stay or lease, is recognized that the original amount authorized will be exceeded, then one (or several) Supplementary Authorizations may be performed. Each Supplementary Authorization completed successfully exceeds to total amount authorized. When the final payment is going to be performed, typically at check-in-out or when finalizing 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. For example, the cardholder did not start fill up the tank with petrol during the assigned time slot or because the cardholder decides to pay with another card during check-out. In this situation a Reversal (Authorization) is initiated in order to release the amount reserved on the cardholders account.

Which “Cardholder Verification Method” (CVM) that shall be used for the particular transaction (e.g. PIN, Signature or No CVM) is determined when performing the Original Authorization.

If PIN is selected, the PIN shall be entered and be verified when performing the Original Authorization (e.g. for a fuel dispenser). As the exact amount is not known when performing the Original Authorization, PIN entry may not be combined with confirmation of the amount as for a “normal” Purchase.

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).

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.

The terminal/PSAM shall not initiate Partial Reversals.

Authorizations and Captures may be geographically and/or time separated.

### 6.3.3 Gratuity and other Cardholder defined Surcharges

Gratuity or other cardholder specified surcharges can be performed after the following principles:

1. The cardholder informs the merchant verbally or by accepting a pre-receipt about any gratuity before the transaction is initiated and the complete transaction processing will be performed based upon the total amount, including gratuity. The Business Call Purchase may be used, when this procedure is used.
2. When the transaction is initiated, the cardholder will via the Cardholder Display, be prompted to decide whether a gratuity shall be added or not. When performing the succeeding PIN entry or printing of the receipt, the total amount including any gratuity will appear. The Business Call Purchase may also be used for this procedure.
3. For signature based transactions the cardholder may add any gratuity when signing the receipt. This principle presumes that the payment is based upon Token based transactions and the receipt is printed after an Original Authorization (and Supplementary Authorization(s), if any), but before the Capture.

The principles 1 and 2 may be performed when the PSAM requests the transaction amount by issuing any variants of the *Get Amount* command. It means that the card has been identified but the transaction processing based on the amount still remain.

### 6.3.4 Card related fees and other Merchant Defined Surcharges

Card fees and other merchant defined surcharges on which the cardholder has no influence, can be added according to the following principles:

1. The merchant or the cash register adds the fee before the transaction is initiated and the complete transaction processing will be performed based upon the total amount, including the fee.
2. For signature based transactions the receipt may indicate the fee(s) and the total transaction amount, which the cardholder approves when signing. This principle presume that the payment is based upon Token based transactions and

the receipt is printed after an Original Authorization (and Supplementary Authorization(s), if any), but before the Capture.

3. For Token based transactions where the cardholder keys in the PIN during the Original Authorization (but do not accept any amounts), merchant related fees may be added before the Capture is initiated and will therefore be indicated on the receipt.

Principle 1 may be performed when the PSAM requests the transaction amount by issuing any variants of the *Get Amount* command. It means that the card has been identified but the transaction processing based on the amount still remain.

### 6.3.5 Cashback

Cashback will be indicated as a subset of the total transaction amount and the indication of cashback is therefore merely used as additional information related to the transaction.

Cashback does not appear on the cardholders display during PIN entry, or the cardholders confirmation of the total amount. But, indication of cashback is required on card related receipts.

Cashback may also appear on the goods & services related receipt, printed by the cash register.

### 6.3.6 Validation, Control and Limitations of Surcharges

When the payment is based upon the transaction types Purchase (and Refund), only *one* transaction amount is conveyed to the PSAM (Cashback may be indicated separate). The amount conveyed is the total transaction amount, including any surcharges and extras.

For Purchase and Refund transactions, it is therefore impossible to perform any control of relationship between goods and services on one hand and surcharges on the other hand (if the amount is transferred before the card is identified).

When the payment is Token based, one or several authorizations (Original Authorization and Supplementary Authorizations) are performed before the concluding Capture.

When the Capture is initiated, the total amount authorized (indicated in the Token used as input for the Capture) as well as the total transaction amount (to be debited the cardholders account) are part of the Capture.

The relationship between the authorized amount and total transaction amount is *not* controlled by the PSAM as specific business rules may apply.

The Merchant Application Handler is the interface to the merchant and therefore also the handler where the transaction

amount is “entered”. If the terminal is integrated with a cash register, the Merchant Application Handler will be the interface to the cash register and thereby the interface to the merchant.

For unattended terminals the merchant will of course be absent, but the automated payment system will functionally act as “merchant”.

If the acquirer defines specific requirements for limitations of surcharges, it will be part of the acquirer agreement signed by each individual merchant.

If any limitations shall be controlled automatically, the specific rules can either be implemented in the cash register/payment system or in the Merchant Application Handler.

In both cases, the requirements for these limitations is outside the scope of this specification.

The present specification defines exclusively technical requirements for the card related part of the payment.

The implementation of such controls in the shops payment systems (and not in the card terminal) gives the following advantages:

- computation of the surcharges and any limitations can be specific for the individual acquirer and/or card types.
- computation of the surcharges and any limitations can be specific for the individual shop/shop segments.

Specific requirements related to the amounts, e.g. rounding of the minor units (or not), selection of currency code or the value of authorization amounts is outside the scope of this specification.

## 6.4 Cardholder Verification

The selection of the CVM (Cardholder Verification Method), i.e. PIN entry, signature or none, is controlled by the PSAM.

### 6.4.1 PIN Entry

PIN entry allows the cardholder to authenticate himself/herself. The PIN length is from 4 to 12 digits, both included.

PIN entry is controlled by the PSAM. The PSAM controls the sequences by calling the PED.

The handling of the entered PIN is also controlled by the PSAM. The entered PIN can be checked online either at the acquirer or at the Issuer via the acquirer.

The entered PIN can for transactions initiated with an ICC be verified off-line in the chip. The PIN can be transmitted to the ICC in plaintext or it can be enciphered.

- 6.4.1.1 B The Terminal shall be able to accept PIN as CVM .

**NOTE:** Depending on the environment, unattended terminals (Terminal Type 25 & 26) may not support PIN.

## 6.4.2 Signature

- 6.4.2.1 A In order to fulfil certain card scheme operating regulations, the Terminal shall be able to accept a signature as CVM.

The PSAM controls this CVM.

- 6.4.2.2 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.

### Signature Verification Function

A Signature Verification functions can be enabled i.e. that the merchant has to validate the cardholder's signature just written on the receipt against the reference signature on the Card. The result of the validation determine the final result of the transaction (approved/declined).

- 6.4.2.3 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.

- 6.4.2.4 A The *Verify Signature* command shall be used to request the merchant for signature verification.

- 6.4.2.5 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:

UNDERSKRIFT OK?  
(Signature OK?)

- 6.4.2.6 A If the Signature Verification function is enabled, but the merchant does not respond positively to the question "UNDERSKRIFT OK?" (Signature OK?), then the transaction shall be voided.

**NOTE:** The PSAM controls this void function.

- 6.4.2.7 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.

### 6.4.3 No CVM

For performance and cost reasons in certain environments neither PIN nor signature is used to verify the cardholders identity.

Such implementations may be relevant where the goods and services are non-transferable and the amount is limited. No CVM may exclude acceptance of certain cards for which PIN or signature is mandatory.

Installation of terminals supporting No CVM requires an individual acceptance from the acquirers including PBS.

## 6.5 Tokens

### 6.5.1 The Use of Tokens

Tokens are used to temporarily store transaction data in a secure manner when a transaction cannot be completed immediately.

A Token is the output when performing the following transaction types:

- Original Authorization
- Supplementary Authorization

A Token is used for input when performing the following transaction types:

- Supplementary Authorization
- Capture
- Reversal (Authorization)

As an example, a cardholder checks in at a hotel and expects to stay there for one week. An Original Authorization transaction is performed with an *estimated amount* for the entire stay. As a result of this transaction, a Token is generated by the PSAM and stored in the backoffice computer in the hotel.

After two nights the cardholder goes to the reception and wants to extend the stay for another week. Then a Supplementary Authorization transaction is performed using an *additional esti-*

*mated amount* to increase the amount authorized. To do this, the original Token is sent to the PSAM along with other transaction data and a new Token is then returned. Again, this Token is stored in the backoffice computer for later use.

When the cardholder checks out, the corresponding Token is used to perform a Capture transaction when the *exact amount* is known. The output from the Capture transaction is a Financial Advice which is stored in the Data Store for later transmission to the acquirer.

- 6.5.1.1 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.
- 6.5.1.2 A A Token shall only be utilized in terminals belonging to the same chain of shops as the terminal that created 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.
- 6.5.1.3 A A Token shall only be utilized in 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 F.83 on page F-69 for further details.
- 6.5.1.4 A Cashback shall not be allowed for Token based transactions.
- 6.5.1.5 A When initiating a Reversal (Authorization), the amount fields in the *Initiate Token Based Payment* command shall be omitted, i.e. that  $LEN_{AMOUNTS} = '00'$ .
- 6.5.1.6 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.
- 6.5.1.7 A Tokens shall be stored (logically) in the Merchant Application.
- 6.5.1.8 B The maximum number of outstanding Tokens handled by the Merchant Application shall match the actual environment e.g. at a gas station, the Merchant Application shall be able to handle as many Tokens at a time as the number of petrol pumps serviced.

### The Format 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 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.

- 6.5.1.9 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 6.10.

### **Retrieval of the Token**

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.

- 6.5.1.10 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 be deleted.

- 6.5.1.11 A Likewise, when a new Token has been created when a Supplementary Authorization has been performed, the old Token shall be deleted.

Table 6.10 – Format of the Token

	Field	Description	Length
I N F O	Token Format	Either 'D2' (EMV), 'D4' (MSC) or 'D6' (Key Entered)	1
	Token version	Binary version number (Initial value: '01')	1
	LEN <sub>AID</sub> + AID/Pre-fix	LEN <sub>AID</sub> + AID with trailing zeroes or first 8 digits of the PAN	17/4
	Accumulated amount	Accumulated amount (binary) of each authorization	4
	CURRC	Currency Code	2
	CURRE	Currency Exponent	1
	VK <sub>CA, TOKEN</sub>	Key version of the PK <sub>CA, TOKEN</sub> used to verify the Token Public Key Certificate (PKC <sub>PSAM, TOKEN</sub> )	1
	VK <sub>TOKEN</sub>	Key version of the CK <sub>TOKEN</sub> 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 <sub>A+B</sub>	Variable used by the PSAM when deciphering the field "Token Data" (LEN <sub>A+B</sub> does <i>not</i> specify the length of the field "Token Data")	2
	Token Data	Token Transaction Data enciphered and signed	
<b>Total</b>			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.			

## 6.6 Multi-Application Driver Handler (MAD-Handler)

### 6.6.1 Printing

- 6.6.1.1 A Receipts shall be printed according to Attachment G.

## 6.7 User Interface Handler

### 6.7.1 Sub–handler, Cardholder Display

#### 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 No CVM 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 9.5 on page 9–10.

The Message Code to be displayed at the Cardholder Display related to a specific Business Call can be found in table 6.11.

Additional information and examples can be found in Attachment M: “Guidelines for Usage of the User Interface Display”

- |         |   |   |
|---------|---|---|
| 6.7.1.1 | A | The display messages shall guide the cardholder through the operational steps of the transaction, e.g. when to insert the card and when enter the PIN.                                    |
| 6.7.1.2 | 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. |

Table 6.11 – 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 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	PIN			'0E' "Wait"	No cardholder interaction
	Signature			'0E' "Wait"	No cardholder interaction
	No CVM			'0E' "Wait"	No cardholder interaction
	Combined			'0E' "Wait"	No cardholder interaction
Capture	PIN			'0E' "Wait"	No cardholder interaction
	Signature			'0E' "Wait"	No cardholder interaction
	No CVM			'0E' "Wait"	No cardholder interaction
	Combined			'0E' "Wait"	No cardholder interaction
Reversal (Authorization)	PIN			'0E' "Wait"	No cardholder interaction
	Signature			'0E' "Wait"	No cardholder interaction
	No CVM			'0E' "Wait"	No cardholder interaction
	Combined			'0E' "Wait"	No cardholder interaction
<b>Legend:</b> 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. "Combined" indicates the CVM consists of PIN & Signature. Grey cells means not applicable.					

- 6.7.1.3 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.
- 6.7.1.4 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”).
- 6.7.1.5 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.
- 6.7.1.6 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.
- 6.7.1.7 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.
- 6.7.1.8 A When an unattended terminal is not able to print a receipt, the dialogue with the cardholder shall give the opportunity (Yes/No) to proceed knowing that no receipt will be printed.
- 6.7.1.9 B When an unattended terminal is able to print a receipt, the dialogue 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.
- 6.7.1.10 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.
- 6.7.1.11 C While the terminal performs application selection, message code ‘0E’ (“Please Wait”) may be displayed on the Cardholder Display.
- 6.7.1.12 B If the card was read successfully but not recognized, Message Code ‘0C’ (“Not Accepted”) shall be displayed on the Cardholder Display.

- 6.7.1.13 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 also be displayed when cardholder confirmation is not requested.

**NOTE:** The text to be displayed may be found in table 6.11 (Business Calls Vs. Message Codes)

The commands send 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.

The transfer (from the MAD-Handler to the User Interface Handler) may e.g. be based on the general *Write Handler String* command. The command may be send 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.

- 6.7.1.14 A The final transaction result based upon the ASW1-ASW2 value shall be displayed on the Cardholder Display.

- 6.7.1.15 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 do not remain in the card reader during the transaction.

- 6.7.1.16 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.

- 6.7.1.17 B When performing
- a Capture or
  - a Supplementary Authorization or
  - a Reversal (Authorization)

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.

- 6.7.1.18 A When the “SLET ALT” (Cancel) key has been activated, message code ‘E7’ (“Purchase interrupted”) shall be displayed on the Cardholder Display.
- 6.7.1.19 C When the receipt is being printed, message code ‘E6’ (“Printing receipt”) shall be displayed on the Cardholder Display.

## 6.7.2 Requirements for PIN Entry State

PIN entry shall only be possible when the Tamper Evident Device (TED), which includes the PIN Pad, is in the PIN Entry State.

The PIN Entry State is initiated when the Tamper Evident Device receives an *Initiate PIN Entry* command.

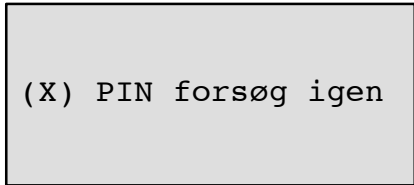
The *Initiate PIN Entry* command is defined in ref. 40: “TAPA, Application Architecture Specification”.

Additional information and examples can be found in Attachment M: “Guidelines for Usage of the User Interface Display”.

The font and position of the messages shown in the figures below are only to be seen as examples.

- 6.7.2.1 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.



(X) PIN forsøg igen

- 6.7.2.2 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 forsøg igen
Forkert PIN
```

- 6.7.2.3 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 forsøg igen
Forkert PIN
Tast PIN
```

- 6.7.2.4 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.

- 6.7.2.5 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.

```
KØB: 123456,78 DKK
PIN: **
(X) PIN forsøg igen

Tast PIN
```

- 6.7.2.6 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").

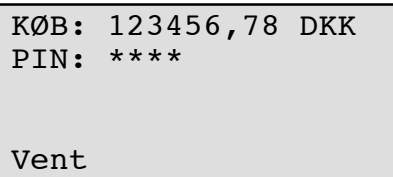
```
KØB: 123456,78 DKK
PIN: ****
(X) PIN forsøg igen

Tast PIN og Godkend
```

**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.

- 6.7.2.7 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").





KØB: 123456,78 DKK  
PIN: \*\*\*\*  
Vent

- 6.7.2.8 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.

## 6.8 Merchant Application Handler

### 6.8.1 Sub-handler, Printer

#### Reports

- 6.8.1.1 A The following reports shall be printed:
- Batch Report
- 6.8.1.2 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.
- 6.8.1.3 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

### 6.8.2 Sub-handler, Merchant Display

- 6.8.2.1 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, 6.8.2.2 and 6.8.2.3, are only relevant for an attended POS Terminal.

6.8.2.2 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.

6.8.2.3 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.

## 6.9 Card Related Transactions

### Transaction flow

Table 6.12 gives a cross reference to the transaction flow figures applicable for specific combinations of Business Calls and sources of transaction data.

An arrow indicates a message between the two handlers (located at the end and at the beginning of the arrow). Handlers in between are not involved.

Dotted lines indicate that the command/response sequence is optional/conditional.

Table 6.12 – Transaction flow figures vs. Business Calls and Sources of Transaction Data

	Purchase	Original Authorization	Supplementary Auth.	Capture	Refund	Reversal
<b>EMV</b>						
PIN	Figure 6.6	Figure 6.9	–	–	–	–
Signature	Figure 6.7	–	–	–	Figure 6.10	–
No CVM	Figure 6.8	Figure 6.9	–	–	–	–
<b>MSC</b>						
PIN	Figure 6.11	Figure 6.14	–	–	–	–
Signature	Figure 6.12	–	–	–	Figure 6.12	–
No CVM	Figure 6.13	Figure 6.15	–	–	–	–
<b>Key Entered</b>						
PIN	–	–	–	–	–	–
Signature	Figure 6.16	–	–	–	Figure 6.16	–
No CVM	Figure 6.17	Figure 6.18	–	–	Figure 6.17	–
<b>Token</b>						
PIN	–	–	–	–	–	–
Signature	–	–	–	Figure 6.20	–	–
No CVM	–	–	Figure 6.19	Figure 6.21	–	Figure 6.22
<b>Legend:</b>						
Figure XX refer to the figure showing the transaction flow for the transaction in question.						
– indicates that the transaction is not applicable.						

## 6.10 EMV Card Transactions

### 6.10.1 Transaction Processing

The terminal must select the card application that is to be used for a particular transaction as defined in section 5.13.5. If the EMV application is selected, then the payment transaction is conducted according to this specification.

The MAD-Handler must engage a dialogue with the consumer and merchant to determine which type of transaction (Purchase, Authorization etc.) is to be performed.

The Merchant Application initiates the transaction by using the appropriate Business Call.

- 6.10.1.1 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.

Figures 6.6 to 6.10 provides examples of typical message flow for successful EMV transactions. For a description of the handlers depicted in the figures, refer to ref. 40: “TAPA, Application Architecture Specification”.

### 6.10.2 Initialization of the EMV Debit/Credit Payment Transaction

- 6.10.2.1 A The MAD-Handler shall frequently poll the Event Handler by sending a *Get Event* command to the Event Handler as defined in ref. 40: “TAPA, Application Architecture Specification”.
- 6.10.2.2 A If the response to the *Get Event* command indicates that a key (Business Call at the Merchant Application) has been pressed, the MAD-Handler shall send a *Read Handler String* command to the Merchant Application in order to get information of the type of Business Call.
- 6.10.2.3 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”.
- 6.10.2.4 A If the terminal displays the message code ‘E0’ (“Terminal Ready”), the terminal shall accept any order of the events (Key Pressed or Card Inserted).

- 6.10.2.5 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 5.13.5 “ICC Application Selection”.
- 6.10.2.6 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.

### 6.10.3 Initiate EMV Payment

The boxes labeled “EMV1” contained in figure 6.6 to figure 6.10 covers the following actions according to ref. 36: “EMV, version 4.1”:

- 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.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 2, the *Initiate EMV Payment 2* command should be utilized.

- 6.10.3.1 A The *Initiate EMV Payment* command shall conform to the format defined in section 8.6.1.
- 6.10.3.2 A The data element “Card Data Source” shall be set to ‘00’ indicating EMV.
- 6.10.3.3 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.
- 6.10.3.4 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 Attachment G, “Receipts”.
- 6.10.3.5 A The data element “TR” (Transaction Request) shall be coded according to the Business Call initiated.
- 6.10.3.6 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).

- 6.10.3.7 A The “Terminal Ident.” (Terminal Identification) shall be coded according to ref. 36: “EMV, version 4.1”.
- 6.10.3.8 A The data element “POS Entry Mode” shall be coded according to Attachment F, section F.9.5.
- 6.10.3.9 A The data element “TT” (Transaction Type) shall be coded according to Attachment F, section F.9.2. Only the 2 most significant digits are indicated in TT.
- 6.10.3.10 B The FCI (File Control Information) returned by a successful selection of the ADF shall be part of the the *Initiate EMV Payment* command, if the total length of the *Initiate EMV Payment* command do 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.
- 6.10.3.11 A If the total length of the *Initiate EMV Payment* exceeds the limit defined in requirement 6.10.3.10, 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.
- 6.10.3.12 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
- 6.10.3.13 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).
- 6.10.3.14 A Counters shall be reported *only* when they have been incremented.
- 6.10.3.15 A The field “Statistics” shall be TLV coded. The tags and format for the different data elements are defined in Attachment F, section F.9.11.

### Entering the Amount

For the Purchase/Refund 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 11.4.2.

6.10.3.16 A The length field LEN<sub>AMOUNTS</sub> shall indicate the appropriate length of all the amount related fields.

6.10.3.17 A In cases where cashback is allowed, this amount (Amount, Other) shall be indicated separately in the *Initiate EMV Payment* command.

It is for to 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 out of scope of this specification.

**NOTE:** The host or PSAM may decline a transaction if the currency is not supported.

6.10.3.18 A For all Original Authorization transactions, the amount shall be included in the *Initiate EMV Payment* command.

### Account Type

6.10.3.19 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 9.2.1 on page 9–2 for further details concerning Account Type.

### PIN Entry

If PIN entry is required as the CVM, the PIN entry must be performed according to ref. 40: “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 over to the MAD–Handler.

The response to the *Initiate EMV Payment* command will conform to the format defined in section 8.6.1.

The Card official name (Card Name), Application Effective Date (DATE<sub>EFFECTIVE</sub>), Application PAN Sequence Number

(PAN<sub>SEQUENCE</sub>) and the Primary Account Number (PAN), all related to the printing of the receipt, will be delivered in the 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 Payment* command.

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.

The Application Status Words (ASW1-ASW2) will indicate the processing status of the *Initiate EMV Payment* command. The possible values of ASW1-ASW2 are defined in table 8.108 to table 8.119.

- 6.10.3.20 A If guidance of the merchant is enabled, the MAD-Handler shall send a *Transaction State Information* command (indicating “Processing”) to the Merchant Application.

#### 6.10.4 EMV Payment

The boxes labeled “EMV2” contained in figure 6.6 to figure 6.10 covers the following actions according to ref. 36: “EMV, version 4.1”:

- Terminal Action Analysis
- Card Action Analysis

These functions are performed by the PSAM.

##### Command

By issuing an *EMV Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

- 6.10.4.1 A The *EMV Payment* command shall conform to the format defined in section 8.6.3.

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.

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.

- 6.10.4.2 A The actual implementation of the Stop List shall not affect the value of the data element Stop List Status.



- 6.10.4.3 A Voice Authorization has priority to validation against a Stop List.
- 6.10.4.4 A An electronic Stop List has priority to validation against a manual Stop List.
- 6.10.4.5 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.
- 6.10.4.6 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 6.5.
- 6.10.4.7 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/Authorisation Code.
- 6.10.4.8 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.
- 6.10.4.9 B If the Merchant Application is configurable based upon a decision that Voice Authorization in general is never feasible, the decision of the actual configuration shall be made by the merchant.
- 6.10.4.10 A When no Approval Code/Authorisation Code has been entered, the field “Approval Code” in the response to the *Check Stop List* command shall be filled with spaces.
- 6.10.4.11 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 Payment* command. The Batch Number will be part of the Financial Requests and Reversals created by the PSAM. See section 6.16.10 for more details concerning the Batch Number.
- 6.10.4.12 A If the MDOL1 (MAD-Handler Data Object List) given in the response to the *Initiate EMV Payment* command indicates that additional data is required, the MAD-Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists.

## 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 8.6.3.

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.

Application Transaction Counter (ATC), related to the printing of the receipt, is part of the response as well.

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 Payment* command.

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.

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 Attachment F.

**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.

- 6.10.4.13 A If an online transaction is requested, the MAD-Handler shall initiate a communication session according to ref. 40: “TAPA, Application Architecture Specification”.

**NOTE:** Initiation of a communication session may be initiated when the MAD-Handler Application has been selected, although the transaction may be completed offline.

- 6.10.4.14 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 online 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.

- 6.10.4.15 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.

- 6.10.4.16 A The ATC to be printed on the receipt shall be taken from the response to the *EMV Payment* command.

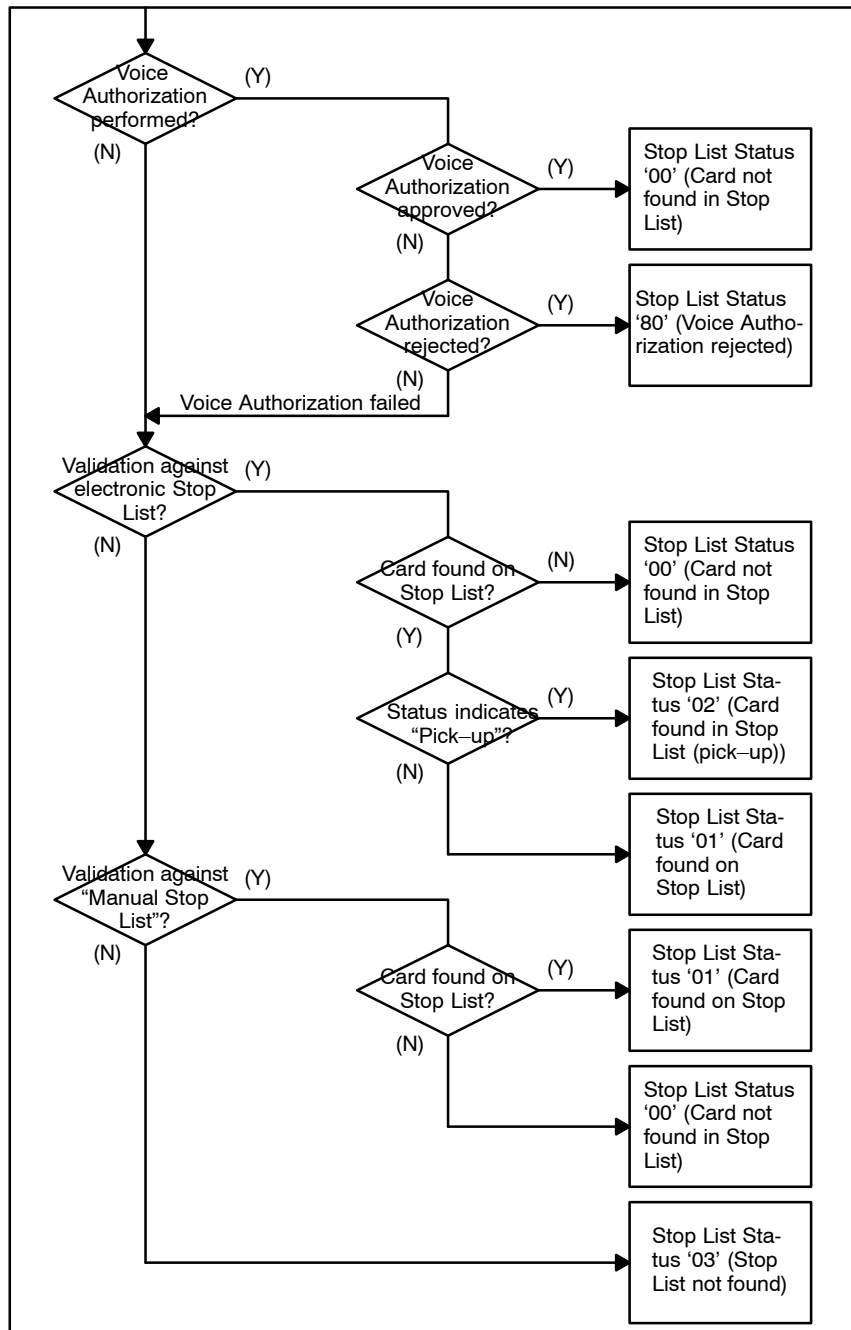


Figure 6.5 – Data Values for Stop List Status

### 6.10.5 Validate Data

The boxes labeled “EMV3” contained in figure 6.6 to figure 6.10 covers the following actions according to ref. 36: “EMV, Version 4.1”:

- Issuer Authentication
- Issuer-to-Card Script Processing

These functions are performed by the PSAM.

**NOTE:** The *Validate Data* command may consist of one or two segments depending of the amount of data.

### Command

By issuing a *Validate Data* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

**NOTE:** The *Validate Data* command may consist of one or two segments depending of the amount of data.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command should be utilized.

- |          |   |  |
|----------|---|--|
| 6.10.5.1 | A | The <i>Validate Data</i> command shall conform to the format defined in section 8.6.4 or 8.6.5.  |
| 6.10.5.2 | A | If the MDOL2 (MAD-Handler Data Object List) given in the response to the <i>EMV Payment</i> command indicates that additional data is required, the MAD-Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists. |
| 6.10.5.3 | 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 Attachment F.  |
| 6.10.5.4 | A | If the terminal has <i>not</i> been online, the length field LEN <sub>HR</sub> shall be set to zero.   |

### Response

When the PSAM has responded to the *Validate Data* command, the application control is returned to the MAD-Handler.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command response should be utilized. For more details concerning the data elements returned and their usage when printing receipts, see Attachment G, “Receipts”.

The response to the *Validate Data* command or *Validate Data 2* will conform to the format defined in section 8.6.4 or 8.6.5.

The Action Code (AC or AC<sub>PRINT</sub>) will inform the MAD-Handler of status of the host response in case of online transaction and the PSAM status in case of an offline transaction.

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.

- 6.10.5.5 A If the “Host Request” data element is present in the response to the *Validate Data* or *Validate Data 2* command, the MAD–Handler shall send the host request and continue the processing from the state where the response to *EMV Payment* command is just received and continue as normal.

**NOTE:** Although the Application Status Words (ASW1–ASW2) indicates declined (e.g. ‘1221’ incorrect PIN), the terminal shall continue as stated in requirement 6.10.5.5.

- 6.10.5.6 C If the response to the *Validate Data* 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. 36: “EMV, version 4.1”.

Scripts may be sent to the ICC, inserted in the Terminal, when the Terminal is on–line.

Scripts are initiated 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.

## 6.10.6 Complete EMV Payment

The boxes labeled “EMV4” contained in figure 6.6 to figure 6.10 covers the following actions according to ref. 36: “EMV, version 4.1”:

- 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.

- 6.10.6.1 A The *Complete EMV Payment* command shall conform to the format defined in section 8.6.6.
- 6.10.6.2 A The data element “Transaction Status” shall be coded according to coding defined for this data element.
- 6.10.6.3 A In case of a signature based transaction if 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 Payment* command, the application control is handed back to the MAD-Handler.

The response to the *Complete EMV Payment* command will conform to the format defined in section 8.6.6.

If the transaction is an Original Authorization, then the response to the *Complete EMV Payment* command will contain a Token.

**NOTE:** Supplementary Authorization is described in section 6.14, “Token Based Transactions”.

- 6.10.6.4 A The MAD-Handler shall convey the Token to Merchant Application by utilizing a *Write Handler String* command to Merchant Application Handler in case of an Original Authorization transaction.
- 6.10.6.5 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.
- 6.10.6.6 A The cardholder shall be informed of the result of the transaction according to the requirement defined in section 5.6.4, “Sub-handler, Cardholder Display” and chapter 10, “Design Requirements”.
- 6.10.6.7 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

The layout of the receipts and the information printed depends on the transaction result and the type of CVM used as stated in Attachment G, “Receipts”.

- 6.10.6.8 A The receipts shall include the parameters identifying the merchant, the terminal and the card as defined in Attachment G, “Receipts”.
- 6.10.6.9 A The MAD-Handler shall initiate printing of a receipt as defined in Attachment G.
- 6.10.6.10 A The PAN shall be part of the receipt printed with some of the digits truncated as stated in Attachment G, “Receipts”.

- 6.10.6.11 A The Card Name to be printed on the receipt shall be taken from (according to the prioritized list):
1. The Application Label (Tag ‘50’) from the ICC (if present)
  2. The response to either an Authorization Request or a Financial Request received from the host (if response received).
  3. The response to the *Initiate EMV Payment* command.
- 6.10.6.12 A The STAN to be printed on the receipt shall be taken from the response to the *Initiate EMV Payment* command.
- 6.10.6.13 A The DATE<sub>EFFECTIVE</sub> to be printed on the receipt shall be taken from the response to the *Initiate EMV Payment* command.
- 6.10.6.14 A If the transaction is signature based and successful, the MAD–Handler shall initiate the final printing of the receipt in order to make it possible for the cardholder to sign a copy the receipt.
- 6.10.6.15 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.
- 6.10.6.16 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.

### 6.10.7 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 MDOL data (MAD–Handler Data Object List data).
- Data elements that must be updateable by the issuer/acquirer and therefore reside in the PSAM (indicated as mandatory (M) in table 6.13).
- Data elements that are conveyed in messages and are therefore stored and maintained inside the PSAM. These data elements are not indicated in table 6.13).
- Data elements that may reside in either the terminal, PSAM or at the acquirer (indicated as optional (O) in table 6.13).

- Data elements listed in table 6.13 are all defined in ref. 36: “EMV, version 4.1”.

**NOTE:** The data elements listed in *italics* in table 6.13 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 6.13 – Storage of Data Elements

Data Element	Reside in PSAM		Reside in Terminal	Updateable (Acquirer/Issuer)	Comments
	M	O			
<i>Acquirer Identifier</i>		*			Added by the acquirer host
<i>Additional Terminal Capabilities</i>			Origin		Conveyed to PSAM <sup>1)</sup>
<i>Amount, Authorized (Binary)</i>	*		Origin		From Merchant Application <sup>2)</sup>
<i>Amount, Other (Binary)</i>	*		Origin		From Merchant Application <sup>2)</sup>
<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 <sup>1)</sup>
<i>Merchant Category Code</i>	*				
<i>Merchant Identifier</i>	*				
<i>Point-of-Service Entry Mode</i>			Origin		Conveyed to PSAM <sup>2)</sup>
<i>Terminal Capabilities</i>			Origin		Conveyed to PSAM <sup>1)</sup>
<i>Terminal Country Code</i>	*				
<i>Terminal Floor Limit</i>	*			*	
<i>Terminal Identification</i>			Origin		Conveyed to PSAM <sup>1)</sup>
<i>Terminal Risk Management Data</i>	*			*	
<i>Terminal Type</i>			Origin		Conveyed to PSAM <sup>1)</sup>
<i>Terminal Verification Results</i>	*				
<i>Transaction Certificate Hash Value</i>	*				
<i>Transaction Currency Code</i>	*		Origin		From Merchant Application <sup>2)</sup>
<i>Transaction Currency Exponent</i>	*		Origin		From Merchant Application <sup>2)</sup>
<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 <sup>2)</sup>
<i>Unpredictable Number</i>	*				

NOTES: <sup>1)</sup> Conveyed in the *Exchange Debit/Credit Static Information* command.  
<sup>2)</sup> Conveyed in the *Initiate EMV Payment* command.

## 6.11 Optimizing the Transaction Time

### 6.11.1 Introduction

In order to speed up the EMV transaction flow when PIN is used as CVM, two different functions are introduced. Depending of the actual card will the PSAM decide whether the basic rules apply or PIN entry may be initiated earlier. The functions are described in details below.

### 6.11.2 Accelerated PIN Entry

The PSAM may perform the Accelerated PIN Entry 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, both of which are described in table 6.14.

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 the 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 the PBS PSAM. The functionality is by default enabled.

If needed, it can be disabled by PBS. It is only possible to disable APE and DAPE for all terminals related to the same ME<sub>NUMBER</sub> – 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 6.14 – 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
	Read Record	Read Record	Initiate PIN Entry
	Read Record	Read Record	Get Processing Options
	•	•	Read Record
	Get Amount	Get KCV	Read Record
	Get KCV	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	Check Stop List	Check Stop List
	1st Generate AC	1st Generate AC	1st Generate AC
Payment	◀		
Validate Data	▶		
	2nd Generate AC	2nd Generate AC	2nd Generate AC
Validate Data	◀		
Complete Paym	▶		
	Add File Record	Add File Record	Add File Record
Complete Paym	◀		
<b>Legend:</b>			
▶ = Command, ◀ = Response, • Additional Read Records may be issued.			

### 6.11.3 Release of the ICC

When the terminal has received the response to the *Validate Data* 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. that neither the display text “Approved”/“Godkendt” nor an audio signal indicating approved may be initiated at this time.

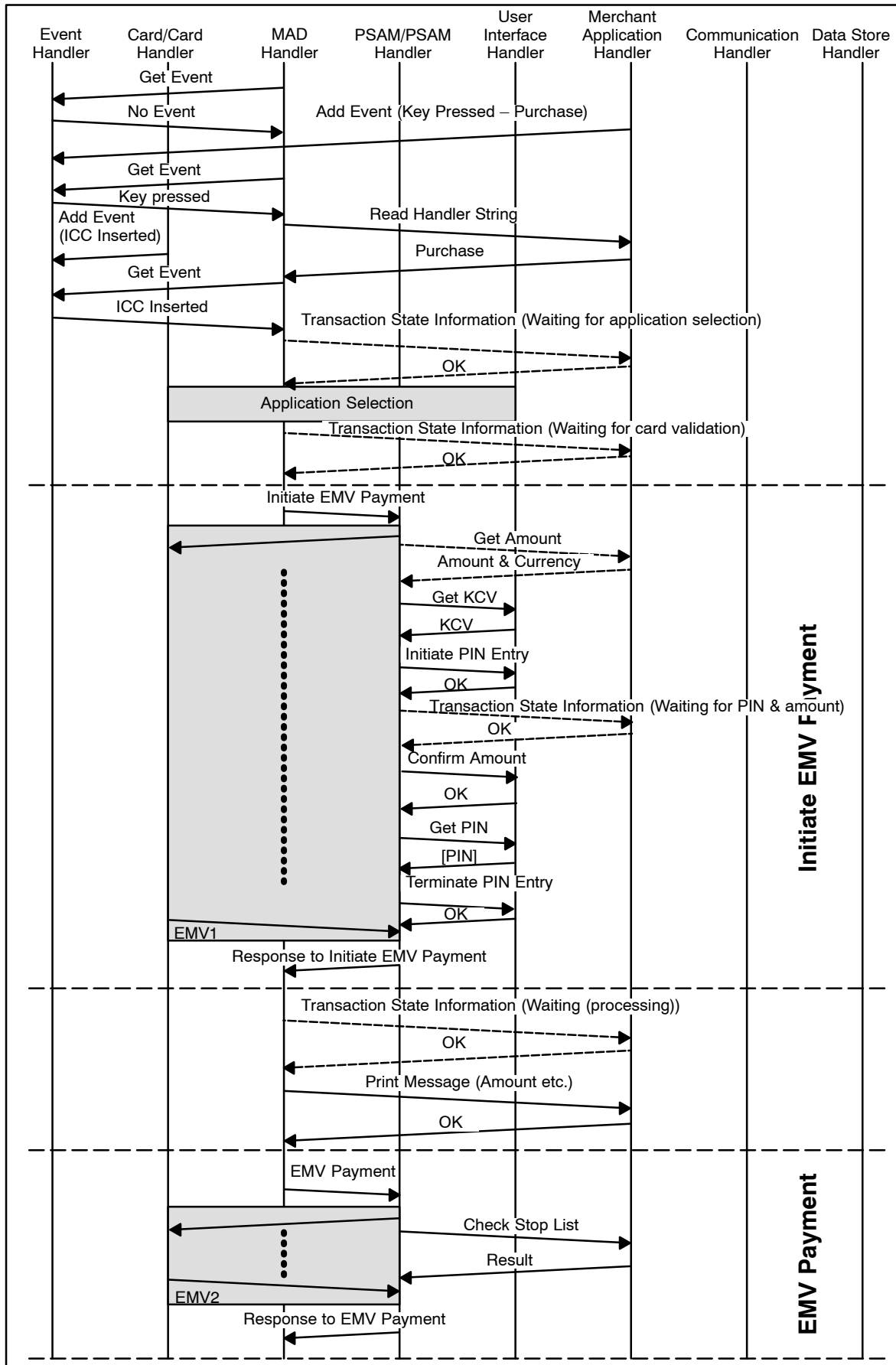


Figure 6.6 – EMV Transaction (Purchase – PIN)

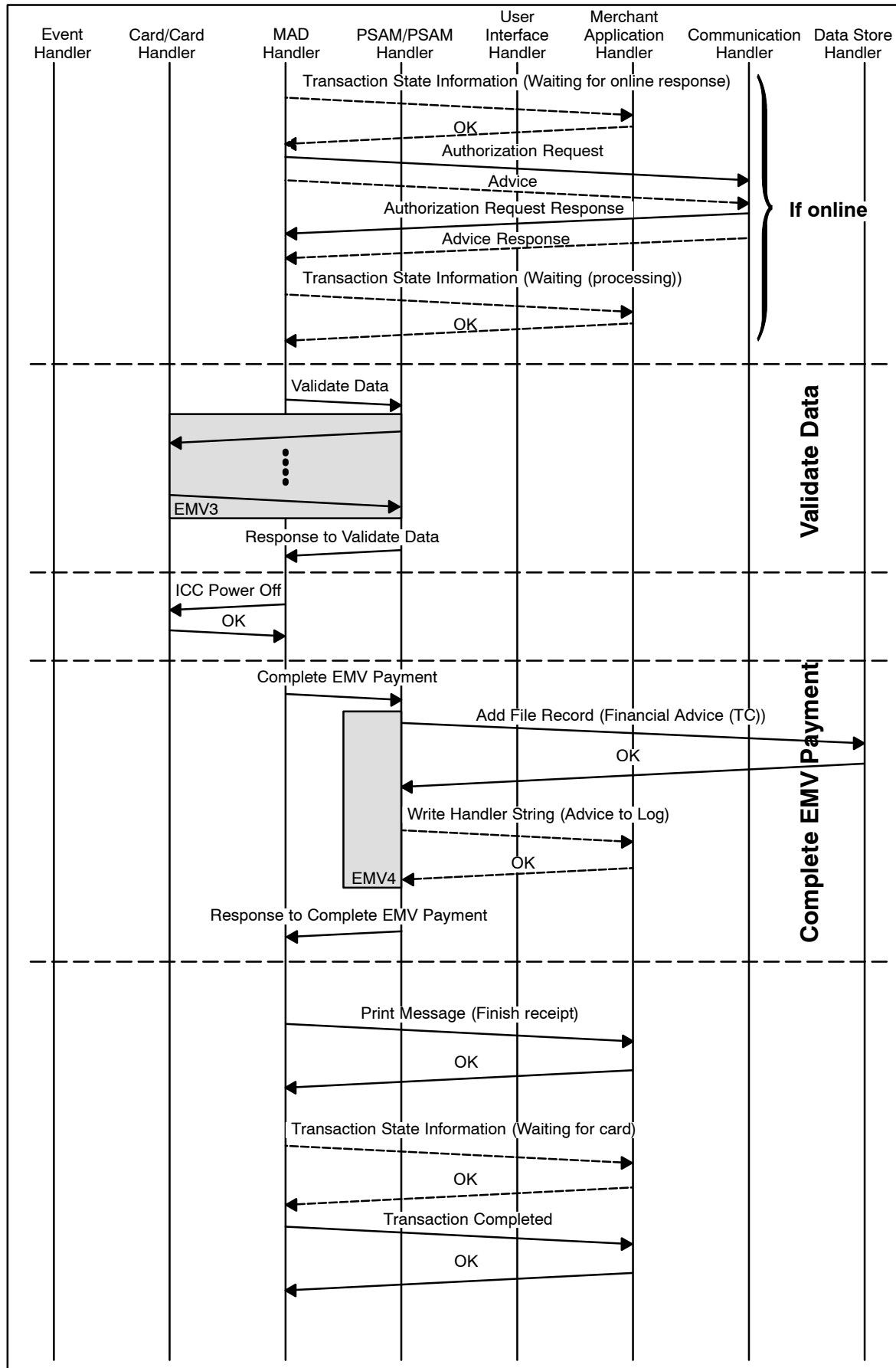


Figure 6.6 – EMV Transaction (Purchase – PIN) (concluded)

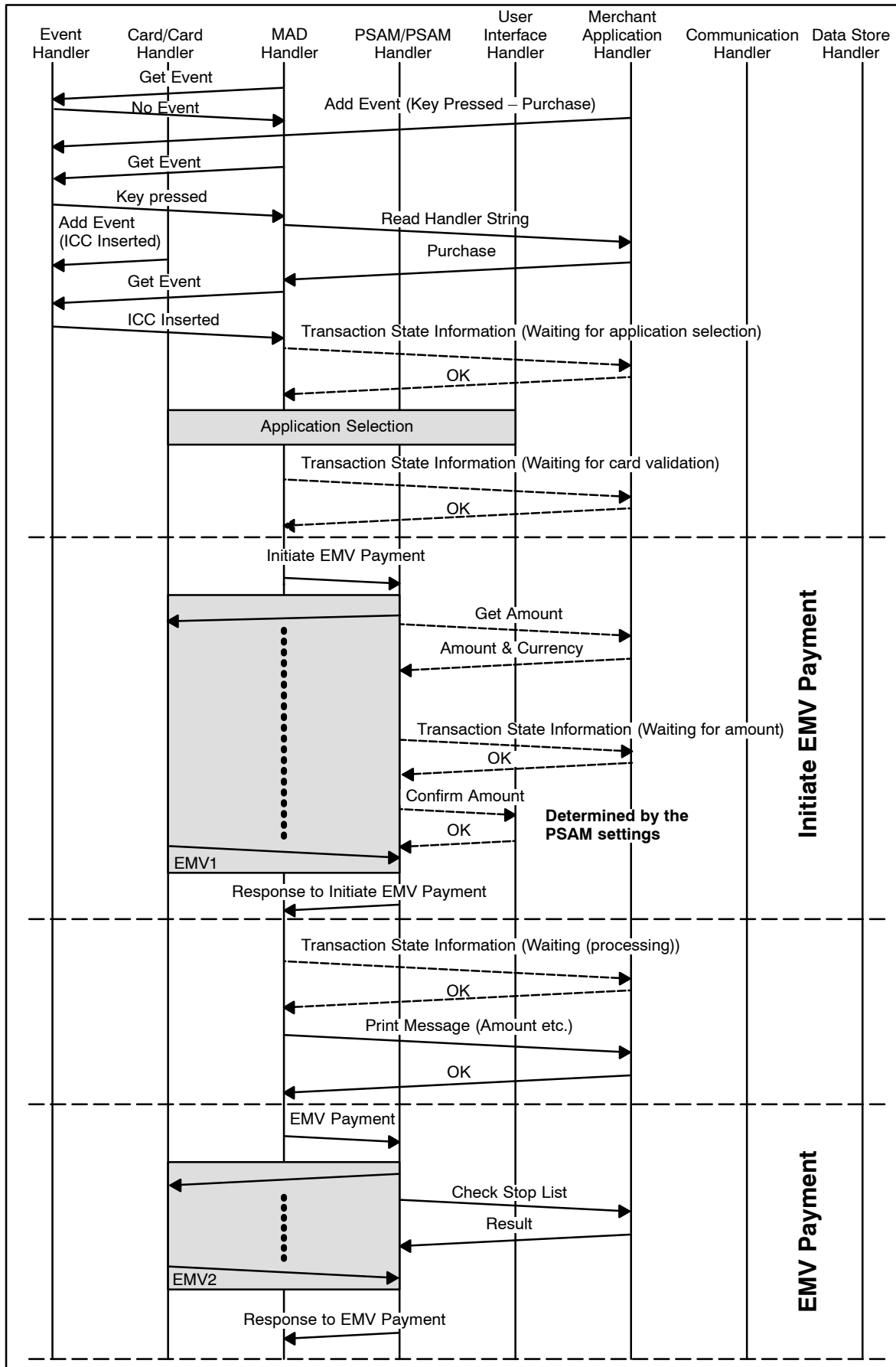


Figure 6.7 – EMV Transaction (Purchase – Signature)

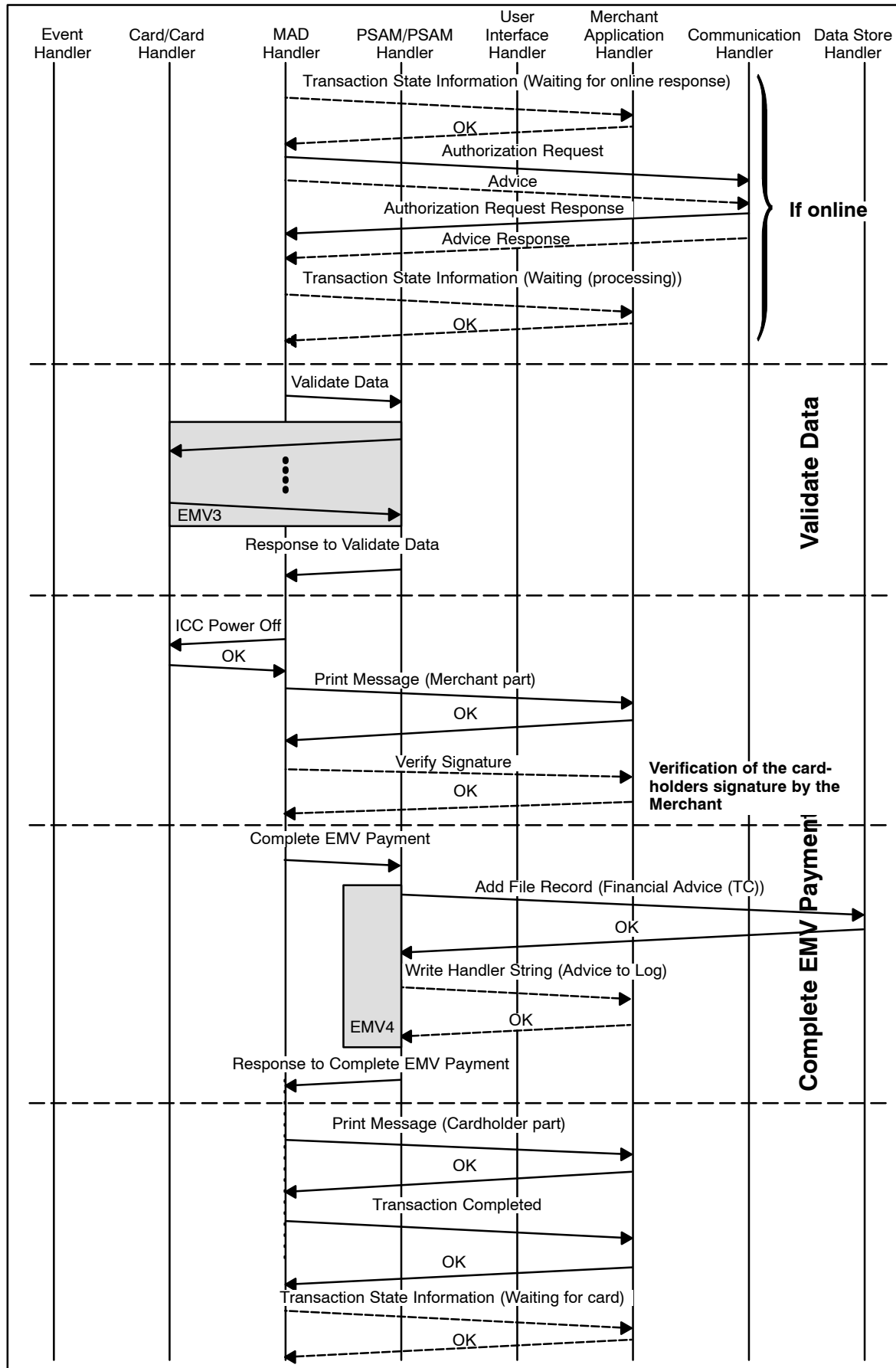


Figure 6.7 – EMV Transaction (Purchase – Signature) (concluded)



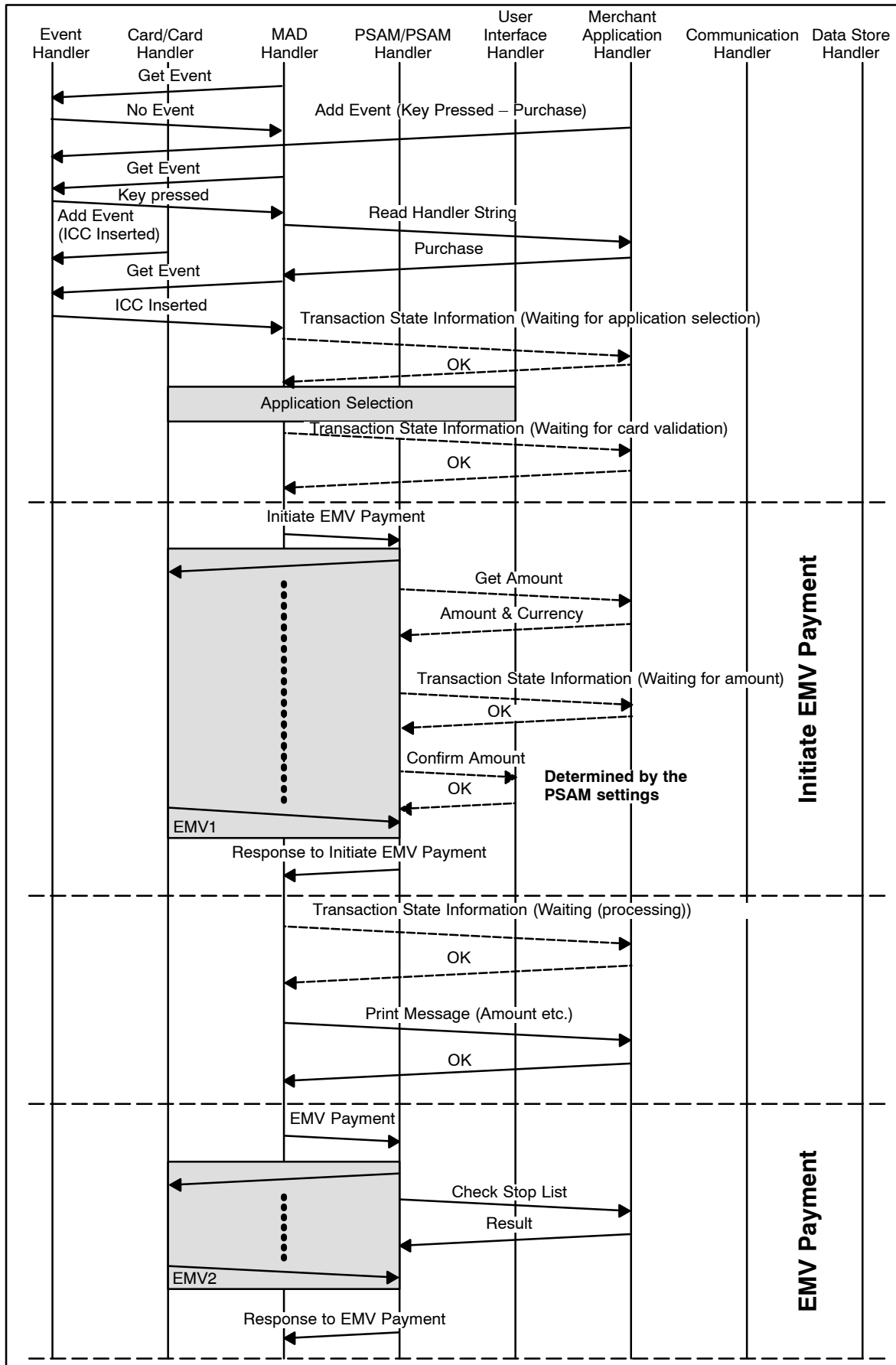


Figure 6.8 – EMV Transaction (Purchase – No CVM)

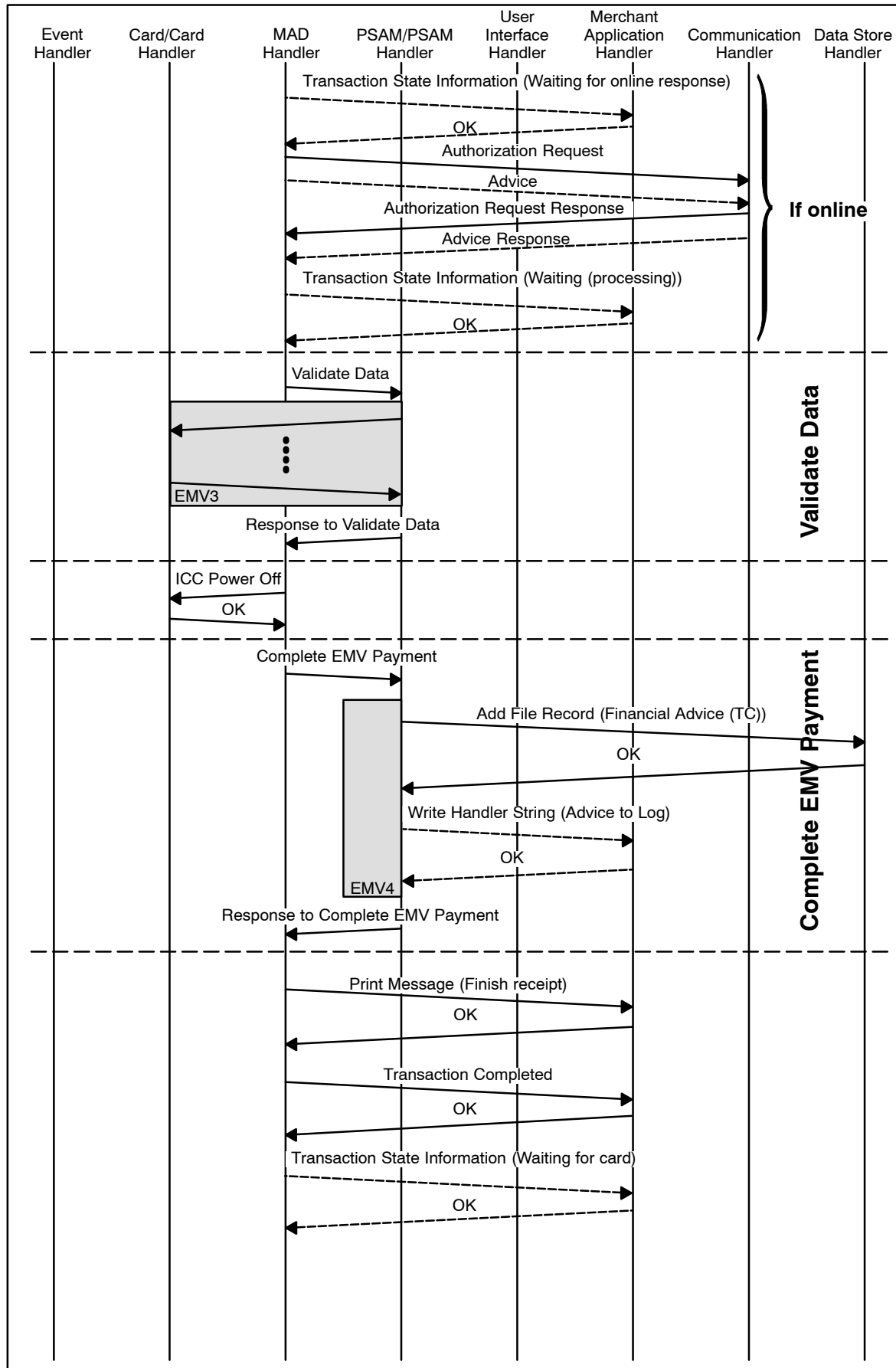


Figure 6.8 – EMV Transaction (Purchase – No CVM) (concluded)

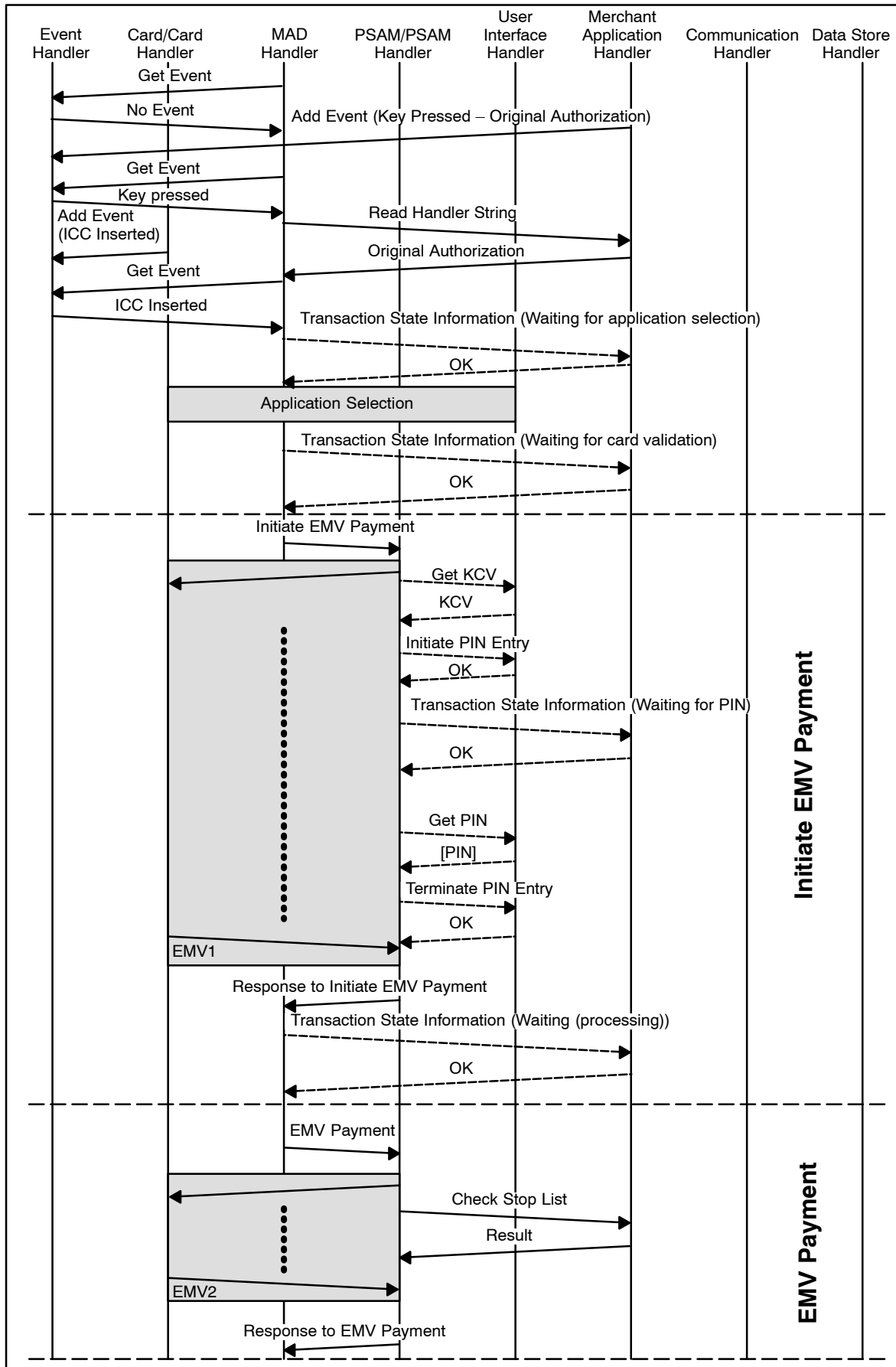


Figure 6.9 – EMV Transaction (Original Authorization – PIN/No CVM)

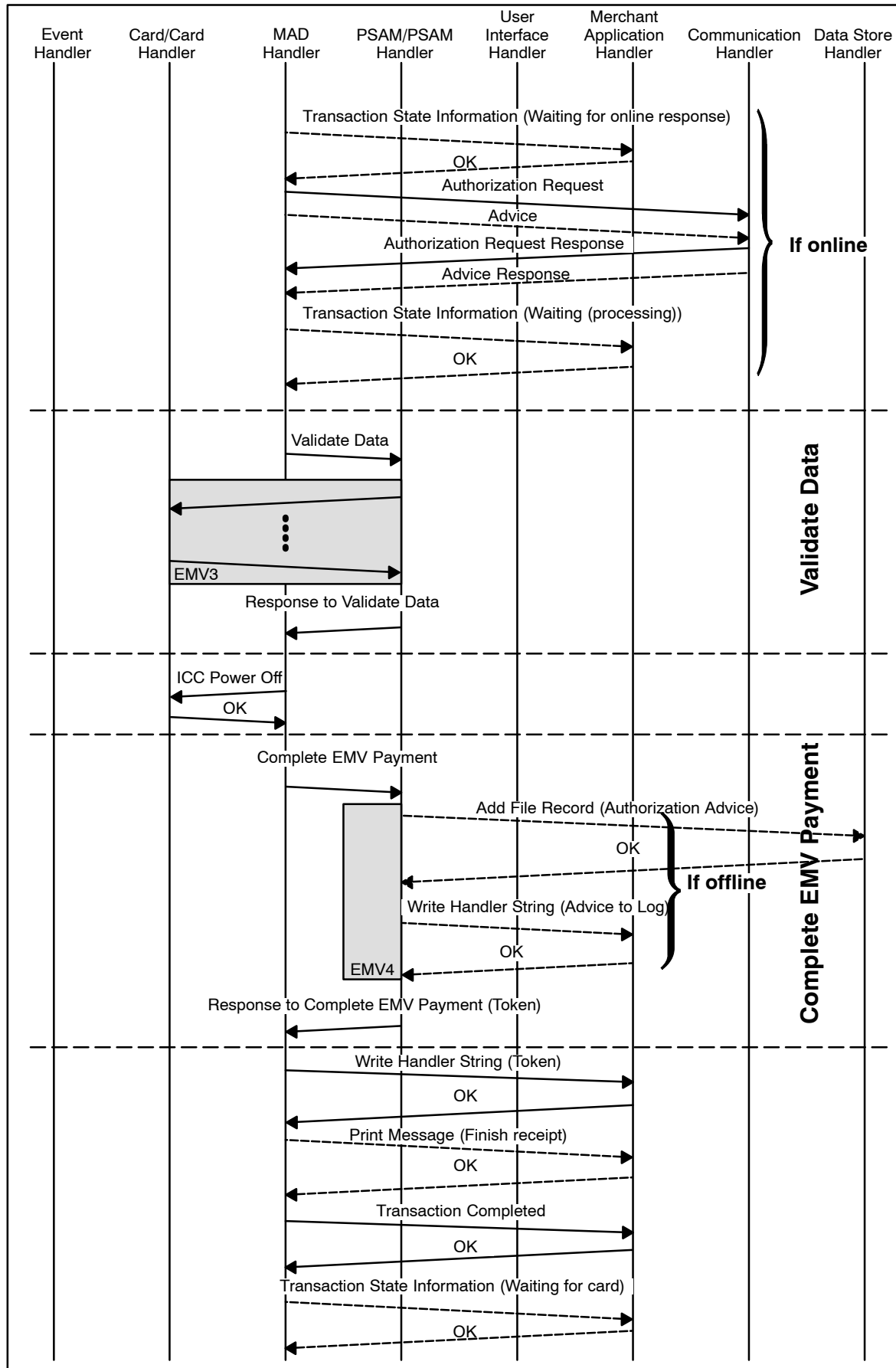


Figure 6.9 – EMV Transaction (Original Authorization – PIN/No CVM) (concluded)

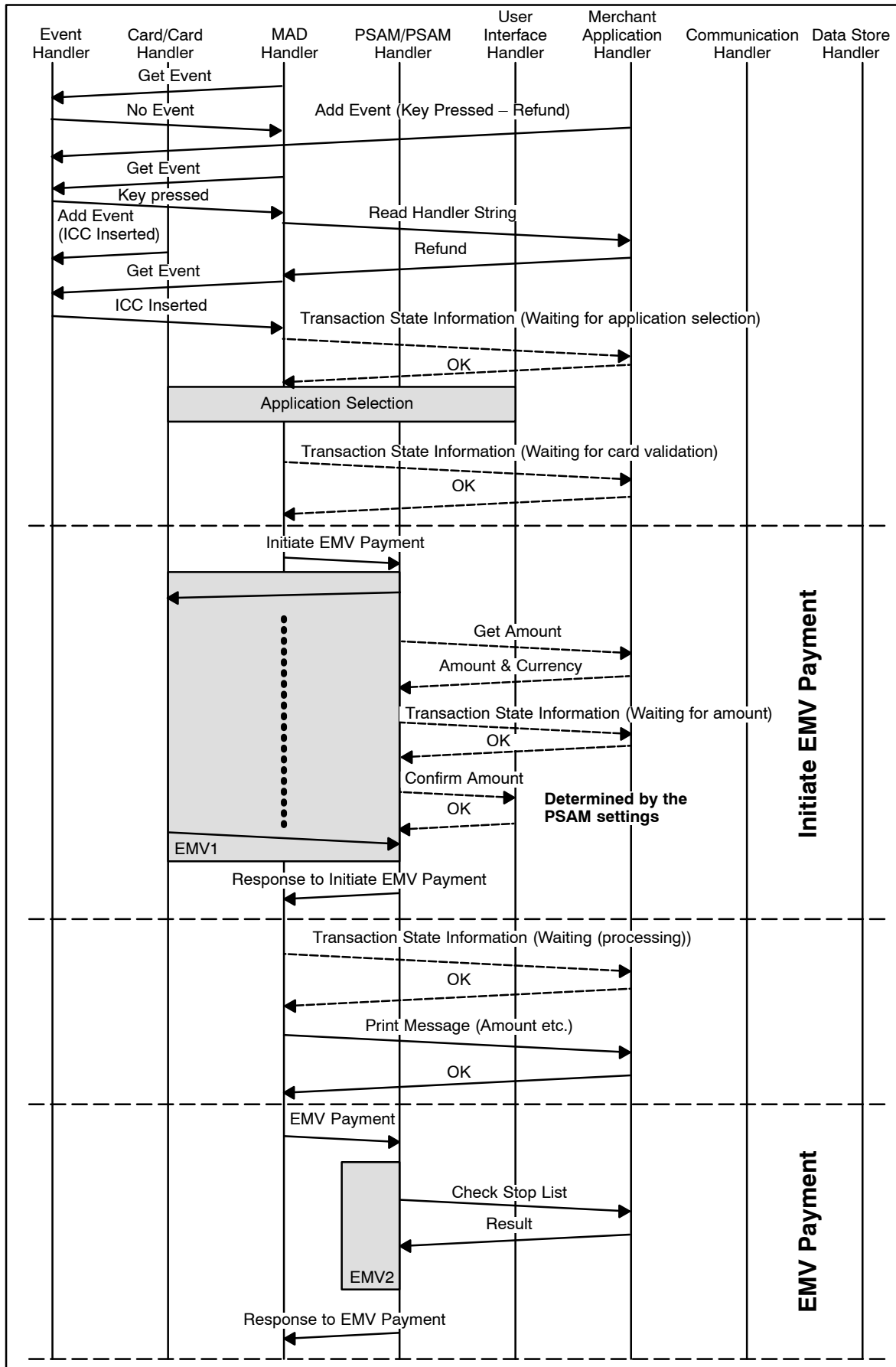


Figure 6.10 – EMV Transaction (Refund – Signature)

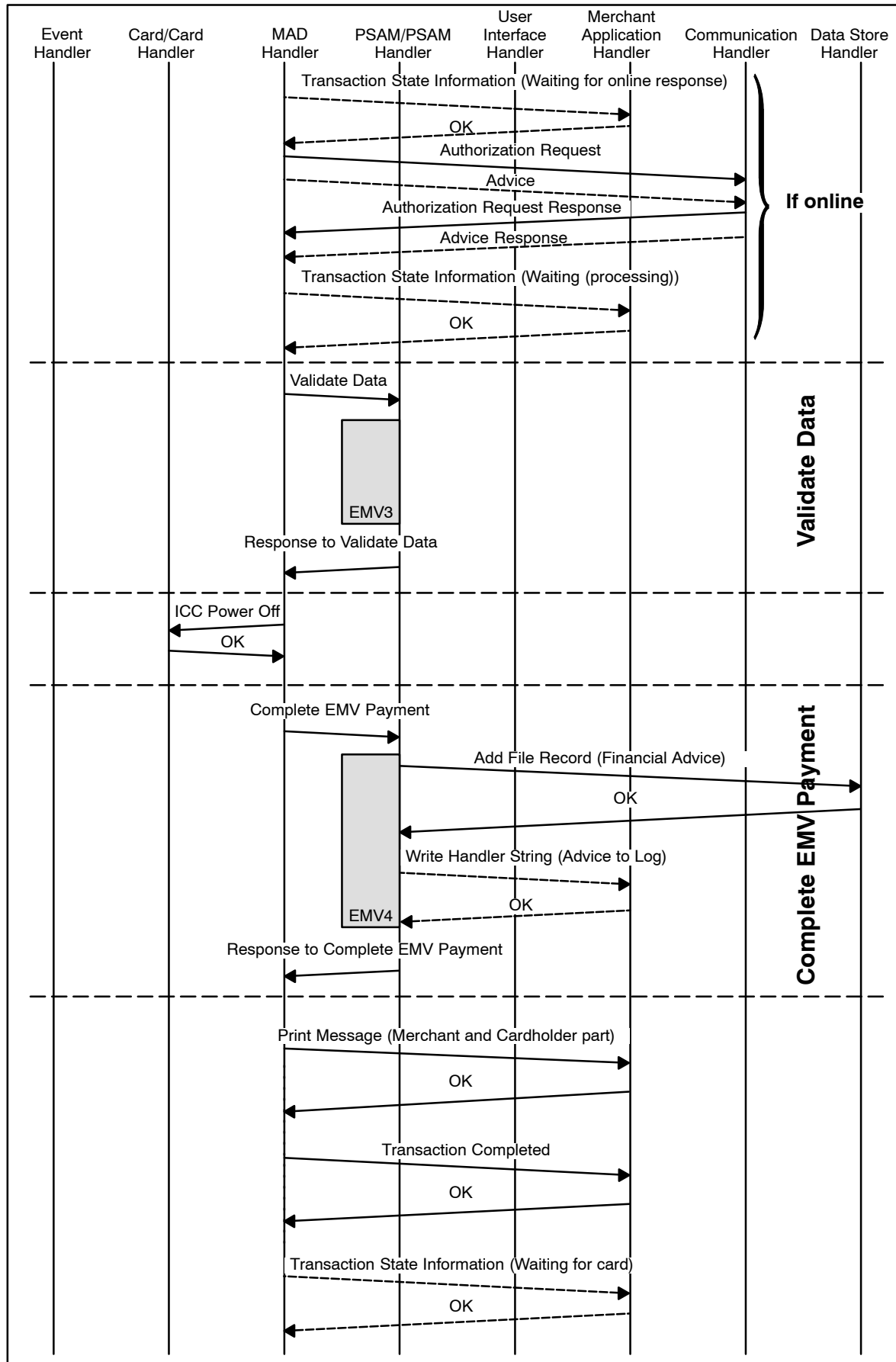


Figure 6.10 – EMV Transaction (Refund – Signature) (concluded)

## 6.12 Magnetic Stripe Card Transactions

### 6.12.1 Transaction Processing

The Merchant Application initiates the transaction by using the appropriate Business Call.

- 6.12.1.1 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.

Figures 6.11 to 6.15 provides examples of typical message flows for successful MSC transactions. For a description of the handlers depicted in the figures, refer to ref. 40: “TAPA, Application Architecture Specification”.

### 6.12.2 Initialization of the MSC Debit/Credit Payment Transaction

- 6.12.2.1 A The MAD–Handler shall frequently poll the Event Handler by sending a *Get Event* command to the Event Handler as defined in ref. 40: “TAPA, Application Architecture Specification”.
- 6.12.2.2 A If the response to the *Get Event* command indicates that a key (Business Call at the Merchant Application) has been pressed, the MAD–Handler shall send a *Read Handler String* command to the Merchant Application in order to get information of the type of Business Call.
- 6.12.2.3 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”.
- 6.12.2.4 A If the terminal displays the message code ‘E0’ (“Terminal Ready”), the terminal shall accept any order of the events (Key Pressed or Card Swiped).
- 6.12.2.5 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 5.13.4 “MSC Application Selection”.
- 6.12.2.6 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.

- 6.12.2.7 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.

### 6.12.3 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.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 2, the *Initiate MSC Payment 2* command should be utilized.

- 6.12.3.1 A The *Initiate MSC Payment* command shall conform to the format defined in section 8.6.7.
- 6.12.3.2 A The data element “Card Data Source” shall be set to ‘01’ indicating MSC.
- 6.12.3.3 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 Attachment G, “Receipts”.
- 6.12.3.4 A The data element “TR” (Transaction Request) shall be coded according to the Business Call initiated.
- 6.12.3.5 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).
- 6.12.3.6 A The “Terminal Ident. (Terminal Identification) shall be coded according to ref. 36: “EMV, version 4.1”.
- 6.12.3.7 A The data element “POS Entry Mode” shall be coded according to Attachment F, section F.9.5.
- 6.12.3.8 A The data element “TT” (Transaction Type) shall be coded according to Attachment F, section F.9.2. Only the 2 most significant digits are indicated in TT.
- 6.12.3.9 A The track 2 data read by the *Read Magnetic Stripe* command shall be conveyed in the data element “TRACK2 DATA”.
- 6.12.3.10 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
- 6.12.3.11 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).
- 6.12.3.12 A Counters shall be reported *only* when they have been incremented.
- 6.12.3.13 A The field “Statistics” shall be TLV coded. The tags and format for the different data elements are defined in Attachment F, section F.9.11.

### Entering the Amount

For the Purchase/Refund 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.

- 6.12.3.14 A The length field LEN<sub>AMOUNTS</sub> shall indicate the appropriate length of all the amount related fields.
- 6.12.3.15 A In cases where cashback is allowed, this amount (Amount, Other) shall be indicated separately in the *Initiate MSC Payment* command.

It is for to the Terminal Supplier to engage a dialogue 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 may decline an online transaction if the currency is not supported by the host.

- 6.12.3.16 A For the Original Authorization transactions, the amount shall included in the *Initiate MSC Payment* command.

It is up to the Terminal Supplier to engage a dialogue 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.

### Account Type

- 6.12.3.17 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 9.2.1 on page 9-2 for further details concerning Account Type.

### PIN Entry

- 6.12.3.18 A If PIN entry is required as the CVM, the PIN entry must be performed according to ref. 40: “TAPA, Application Architecture Specification”.

### Response

When the PSAM has responded to the *Initiate MSC Payment* command, the application control is returned over to the MAD-Handler.

The response to the *Initiate MSC Payment* command will conform to the format defined in section 8.6.7.

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 MSC Payment* command.

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.

- 6.12.3.19 A The STAN to be printed on the receipt shall be taken from the response to the *Initiate MSC Payment* command.

The Application Status Words (ASW1-ASW2) will indicate the processing status of the *Initiate MSC Payment* command. The possible values of ASW1-ASW2 are defined in table 8.108 to table 8.119.

- 6.12.3.20 A If guidance of the merchant is enabled, the MAD-Handler shall send a *Transaction State Information* command (indicating “Processing”) to the Merchant Application.

## 6.12.4 MSC Payment

### Command

By issuing an *MSC Payment* command to the PSAM, application control is handed over from the MAD-Handler to the PSAM.

- 6.12.4.1 A The *MSC Payment* command shall conform to the format defined in section 8.6.9.

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.

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.

6.12.4.2 A The actual implementation of the Stop List shall not affect the value of the data element Stop List Status.

6.12.4.3 A Voice Authorization has priority to validation against a Stop List.

6.12.4.4 A An electronic Stop List has priority to validation against a manual Stop List.

6.12.4.5 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.

6.12.4.6 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 6.5.

The selection value for Stop List Status, as defined by the requirements above, may be expressed by figure 6.5.

6.12.4.7 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/Authorisation Code.

6.12.4.8 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.

6.12.4.9 B If the Merchant Application is configurable based upon a decision that Voice Authorization in general is never feasible, the decision of the actual configuration shall be made by the merchant.

- 6.12.4.10 A If the card does not appear on the Stop List and the Voice Authorization is rejected, the “Stop List Status” shall be set to ‘80’.
- 6.12.4.11 A When no Approval Code/Authorisation Code has been entered, the field “Approval Code” in the response to the *Check Stop List* command shall be filled with spaces.
- 6.12.4.12 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 *MSC Payment* command. The Batch Number will be part of the Financial Requests and Reversals created by the PSAM. See section 6.16.10 for more details concerning the Batch Number.
- 6.12.4.13 A If the MDOL1 (MAD-Handler Data Object List) given in the response to the *Initiate MSC Payment* command indicates that additional data is required, the MAD-Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists.

### 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 8.6.9.

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 *MSC Payment* command.

If the PSAM has determined that an online transaction is required, the PSAM will return a complete (inclusive APACS header) Financial Request or Authorization Request according to Attachment F.

- 6.12.4.14 A If an online transaction is requested, the MAD-Handler shall initiate a communication session according to ref. 40: “TAPA, Application Architecture Specification”.
- 6.12.4.15 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.

- 6.12.4.16 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.

## 6.12.5 Validate Data

### Command

By issuing a *Validate Data* command to the PSAM, application control is handed over from the MAD–Handler to the PSAM.

**NOTE:** The *Validate Data* command may consist of one or two segments depending of the amount of data.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command should be utilized.

- 6.12.5.1 A The *Validate Data* or *Validate Data 2* command shall conform to the format defined in section 8.6.4 or 8.6.5.
- 6.12.5.2 A If the MDOL2 (MAD–Handler Data Object List) given in the response to the *MSC Payment* command indicates that additional data is required, the MAD–Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists.
- 6.12.5.3 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 Attachment F.
- 6.12.5.4 A If the terminal has *not* been online, the length field LEN<sub>HR</sub> shall be set to zero.

### Response

When the PSAM has responded to the *Validate Data* command, the application control is returned to the MAD–Handler.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command response should be utilized. For more details concerning the data elements returned and their usage when printing receipts, see Attachment G, “Receipts”.

The response to the *Validate Data* or *Validate Data 2* command will conform to the format defined in section 8.6.4 or 8.6.5.

The Action Code (AC or AC<sub>PRINT</sub>) will inform the MAD–Handler of status of the host response in case of online transaction and the PSAM status in case of an offline transaction.

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.

- 6.12.5.5 A If the “Host Request” data element is present in the response to the *Validate Data* or *Validate Data 2* command, the MAD-Handler shall send the host request and continue the processing from the state where the response to *MSC Payment* command is just received and continue as normal.

**NOTE:** Although the Application Status Words (ASW1-ASW2) indicates declined (e.g. ‘1221’ incorrect PIN), the terminal shall continue as stated in requirement 6.12.5.5.

## 6.12.6 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.

- 6.12.6.1 A The *Complete Payment* command shall conform to the format defined in section 8.6.10.
- 6.12.6.2 A The data element “Transaction Status” shall be coded according to the coding defined for this data element.
- 6.12.6.3 A In case of a signature based transaction if 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 Payment* command, the application control is handed back to the MAD-Handler.

The response to the *Complete Payment* command will conform to the format defined in section 8.6.10.

If the transaction is an Original Authorization, then the response to the *Complete Payment* command will contain a Token as defined in section 6.5.

**NOTE:** Supplementary Authorization is described in section 6.14, “Token Based Transactions”.

- 6.12.6.4 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 Authorization transaction.
- 6.12.6.5 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.
- 6.12.6.6 A The cardholder shall be informed of the result of the transaction according to the requirement defined in section 5.6.4, “Sub–handler, Cardholder Display” and chapter 10, “Design Requirements”.
- 6.12.6.7 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

The layout of the receipts and the information printed depends on the transaction result and the type of CVM used as stated in Attachment G, “Receipts”.

- 6.12.6.8 A The receipts shall include the parameters identifying the merchant, the terminal and the card as defined in Attachment G, “Receipts”.
- 6.12.6.9 A The MAD–Handler shall initiate printing of a receipt as defined in Attachment G.
- 6.12.6.10 A The PAN shall be part of the receipt printed with some of the digits truncated as stated in Attachment G, “Receipts”.
- 6.12.6.11 A The STAN to be printed on the receipt shall be taken from the response to the *Initiate MSC Payment* command or from the response to the *Validate Data* command in case of PIN retry.
- 6.12.6.12 A If a response to either an Authorization Request or a Financial Request is received from the host, the Card Name to be printed on the receipt shall be taken from this response. If no response is received, the Card Name to be printed on the receipt shall be taken from the response to the *Initiate MSC Payment* command.
- 6.12.6.13 A If the transaction is signature based and successful, the MAD–Handler shall initiate the final printing of the receipt in order to make it possible for the cardholder to sign a copy the receipt.

6.12.6.14 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.

6.12.6.15 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.



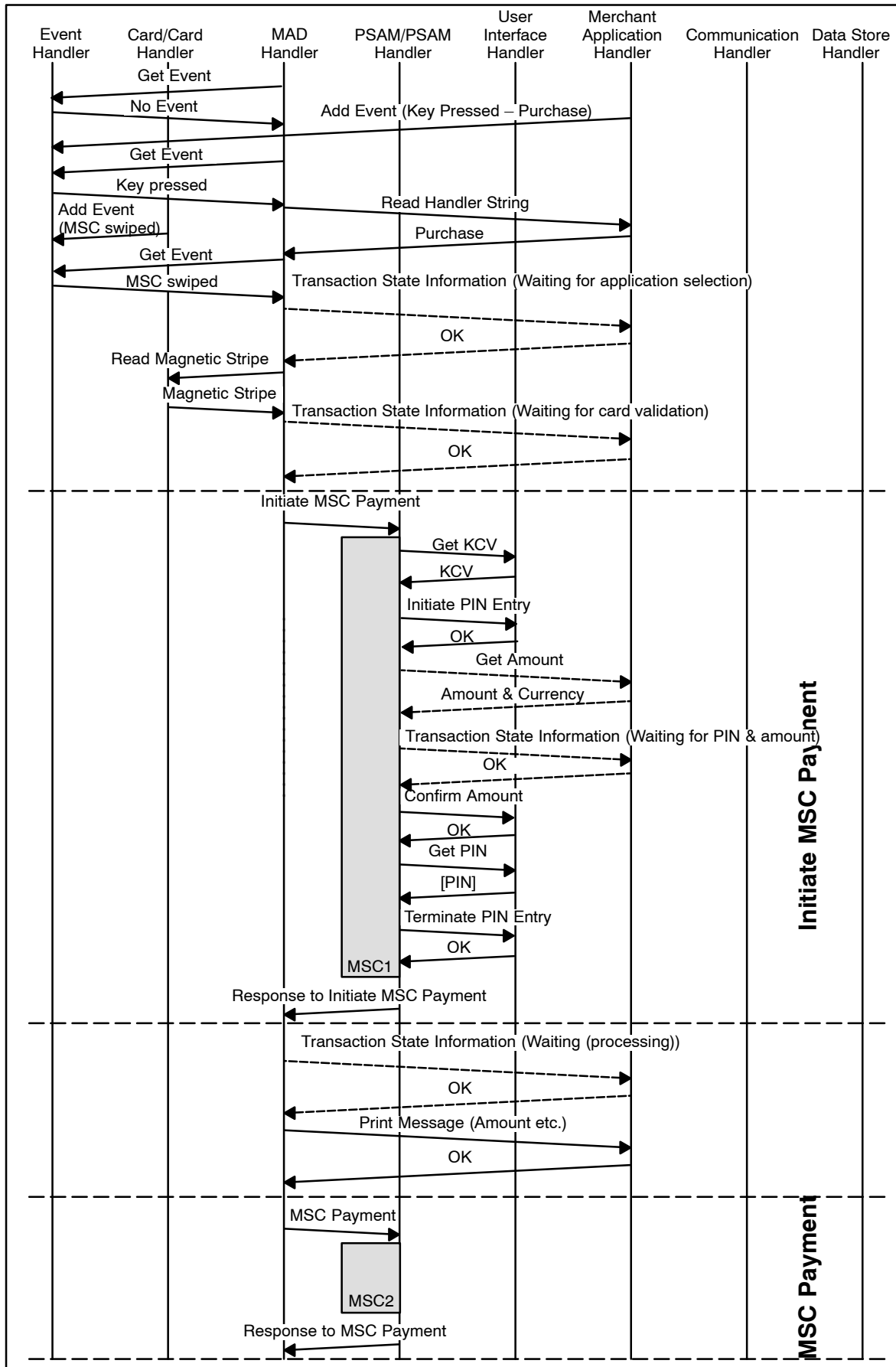


Figure 6.11 – MSC Transaction (Purchase – PIN)

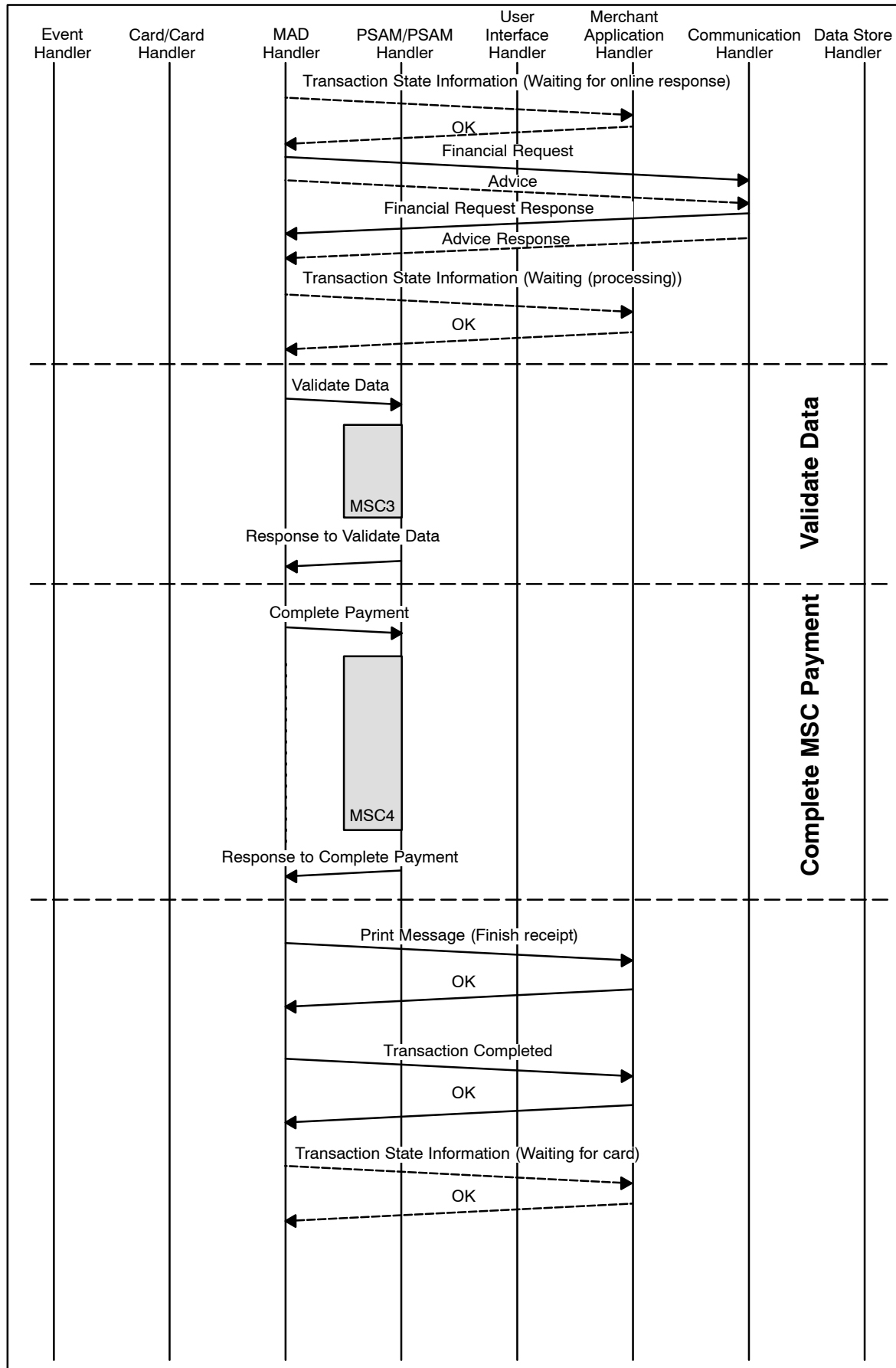


Figure 6.11 – MSC Transaction (Purchase – PIN) (concluded)

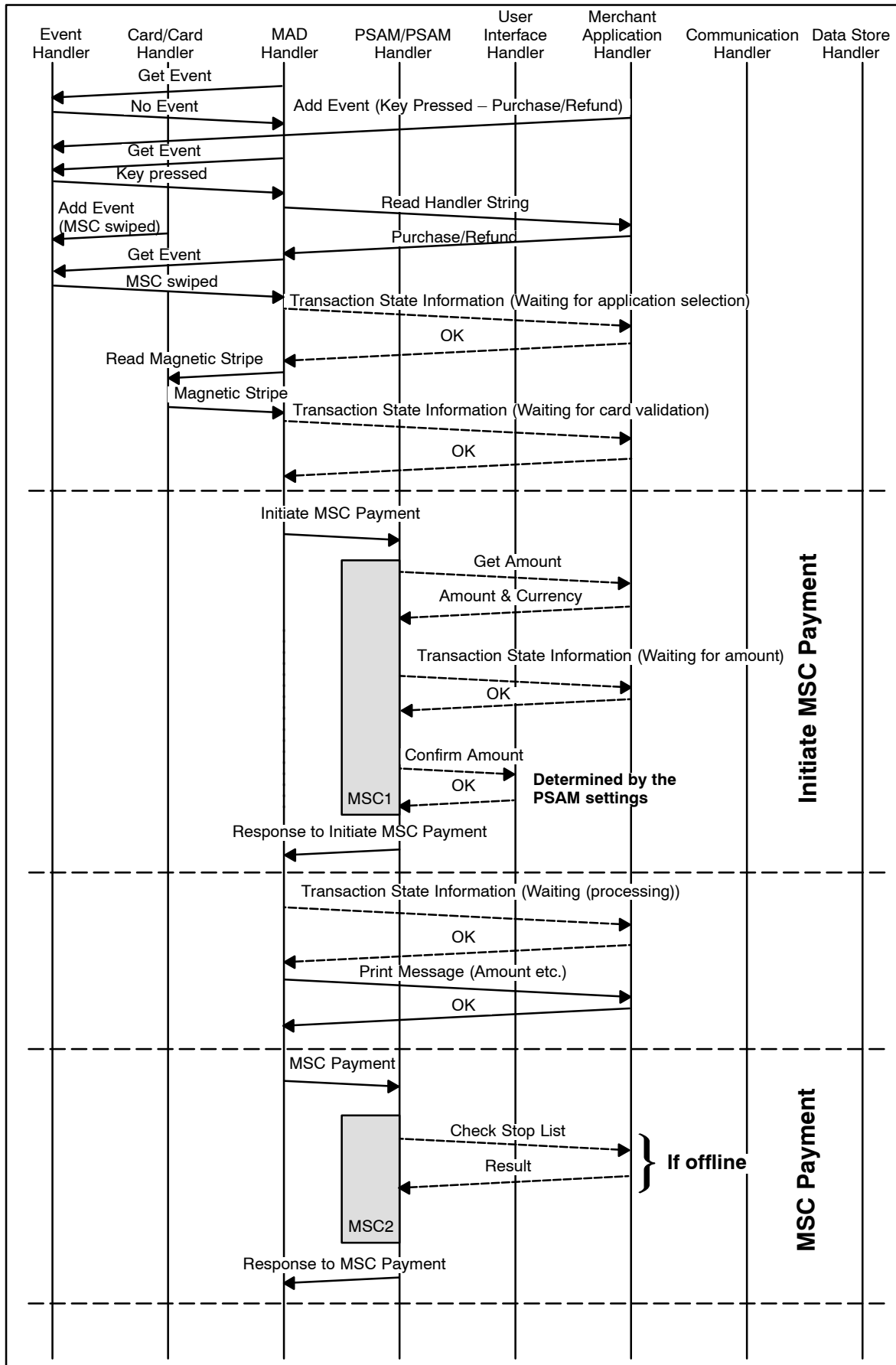


Figure 6.12 – MSC Transaction (Purchase/Refund – Signature)

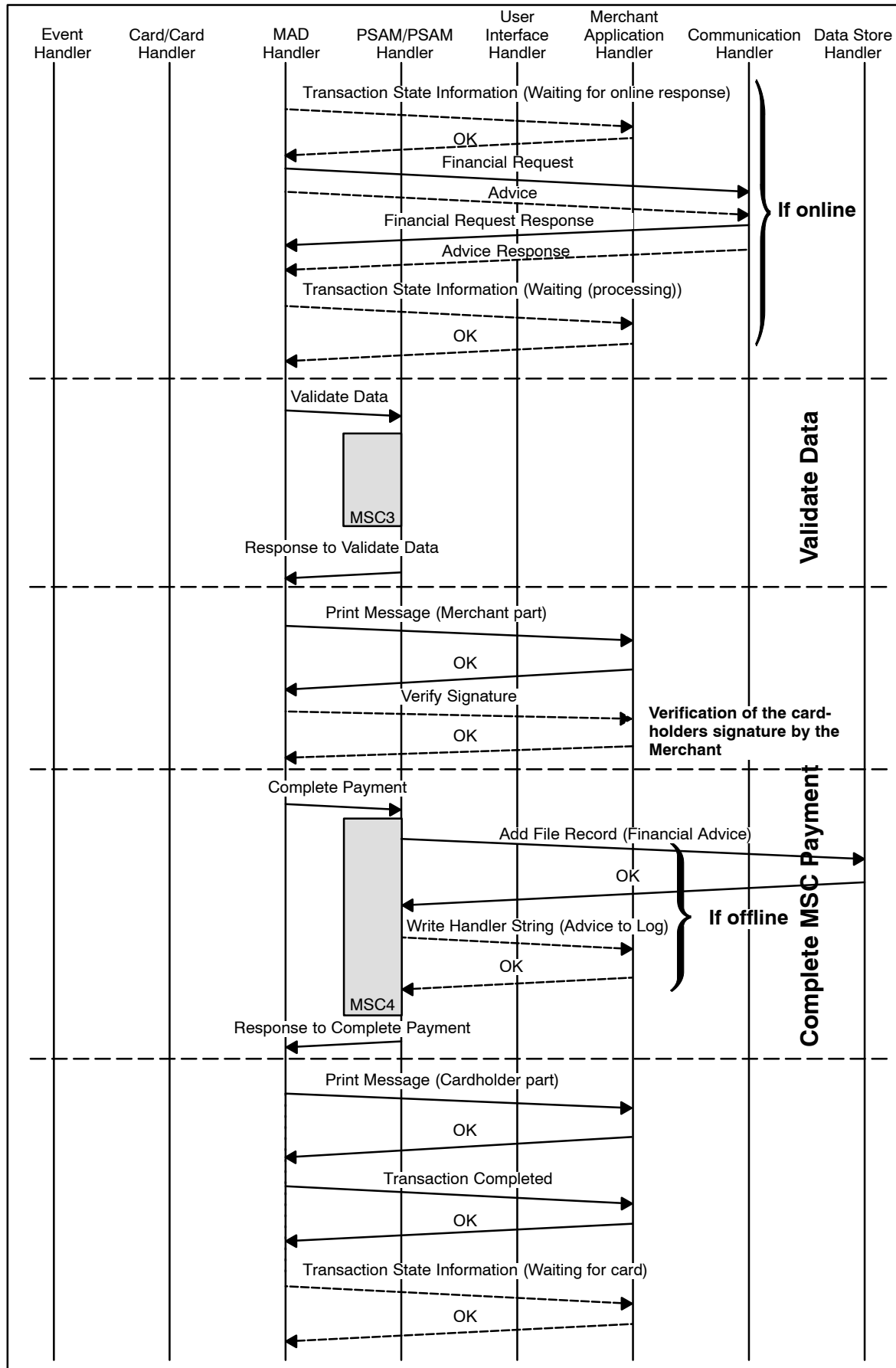


Figure 6.12 – MSC Transaction (Purchase/Refund – Signature) (concluded)

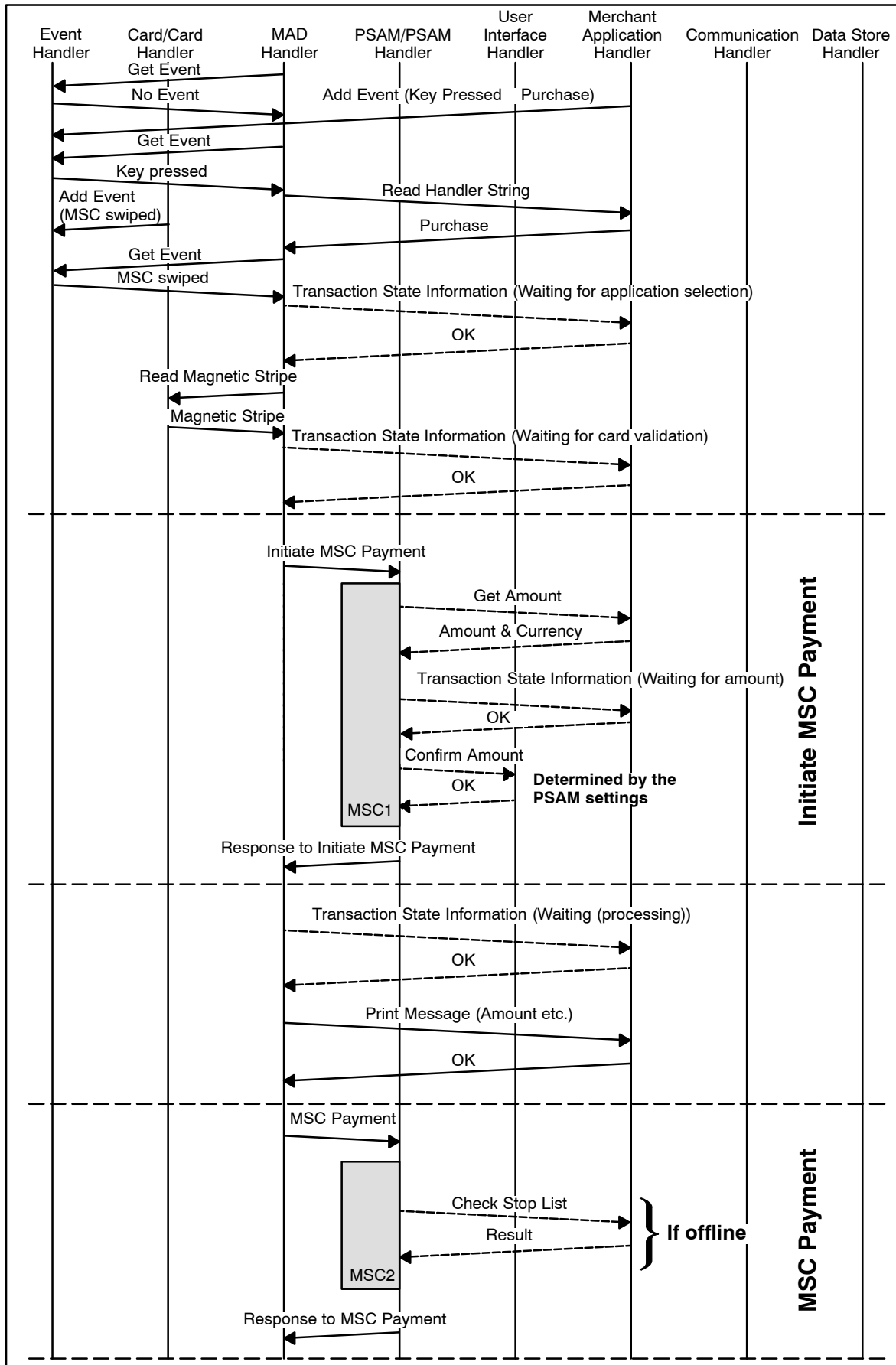


Figure 6.13 – MSC Transaction (Purchase – No CVM)

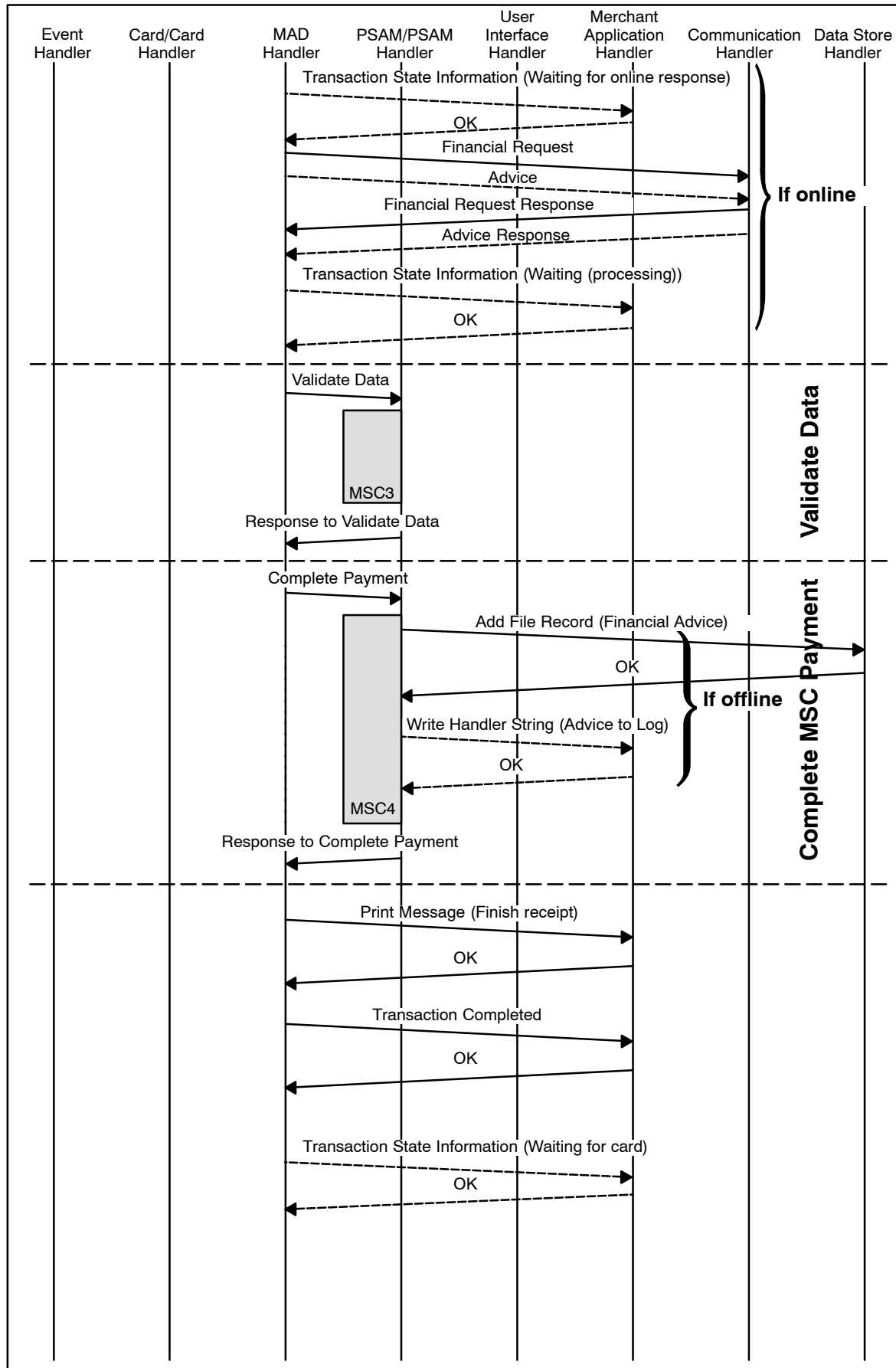


Figure 6.13 – MSC Transaction (Purchase – No CVM) (concluded)

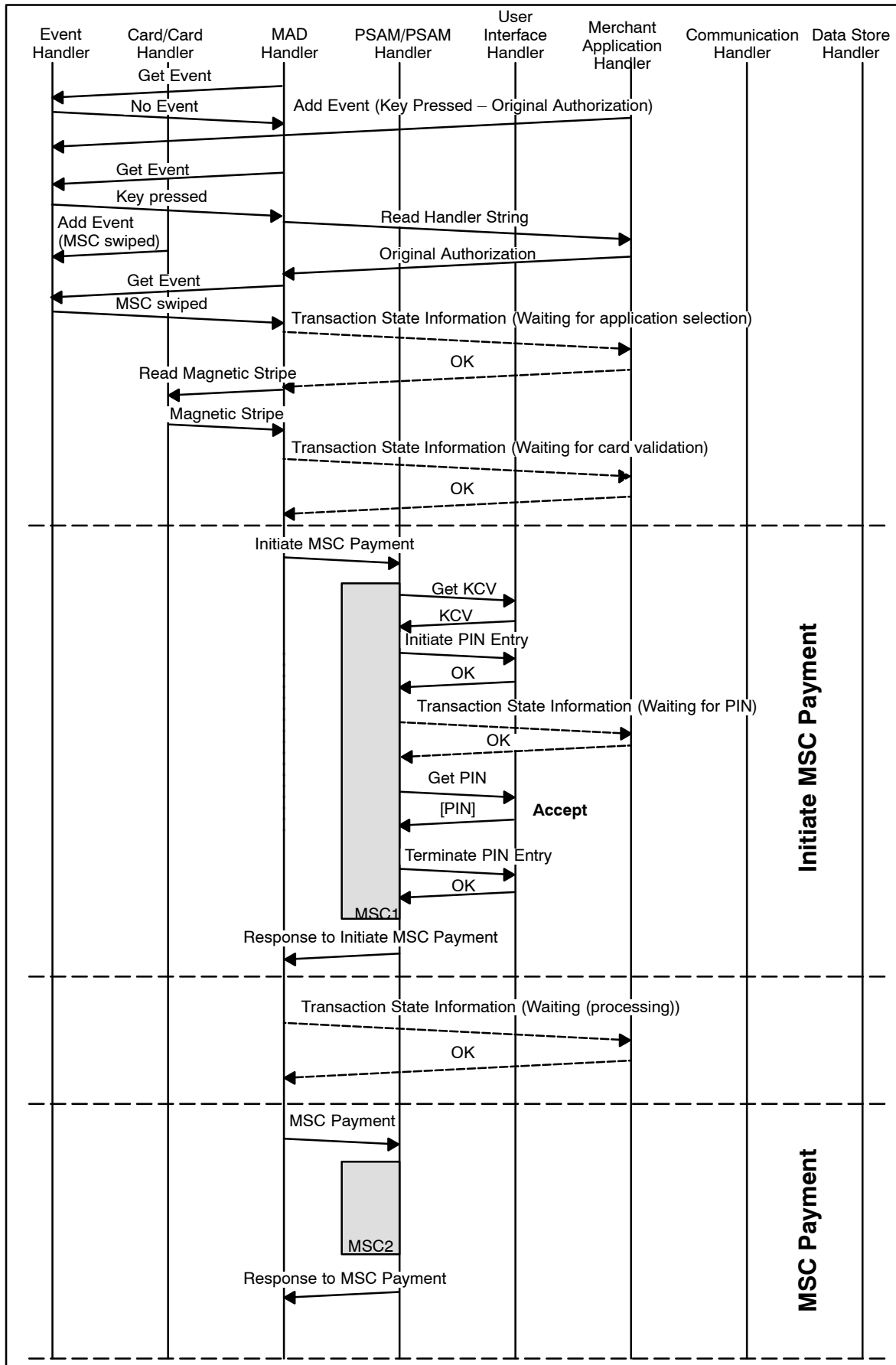


Figure 6.14 – MSC Transaction (Original Authorization – PIN)

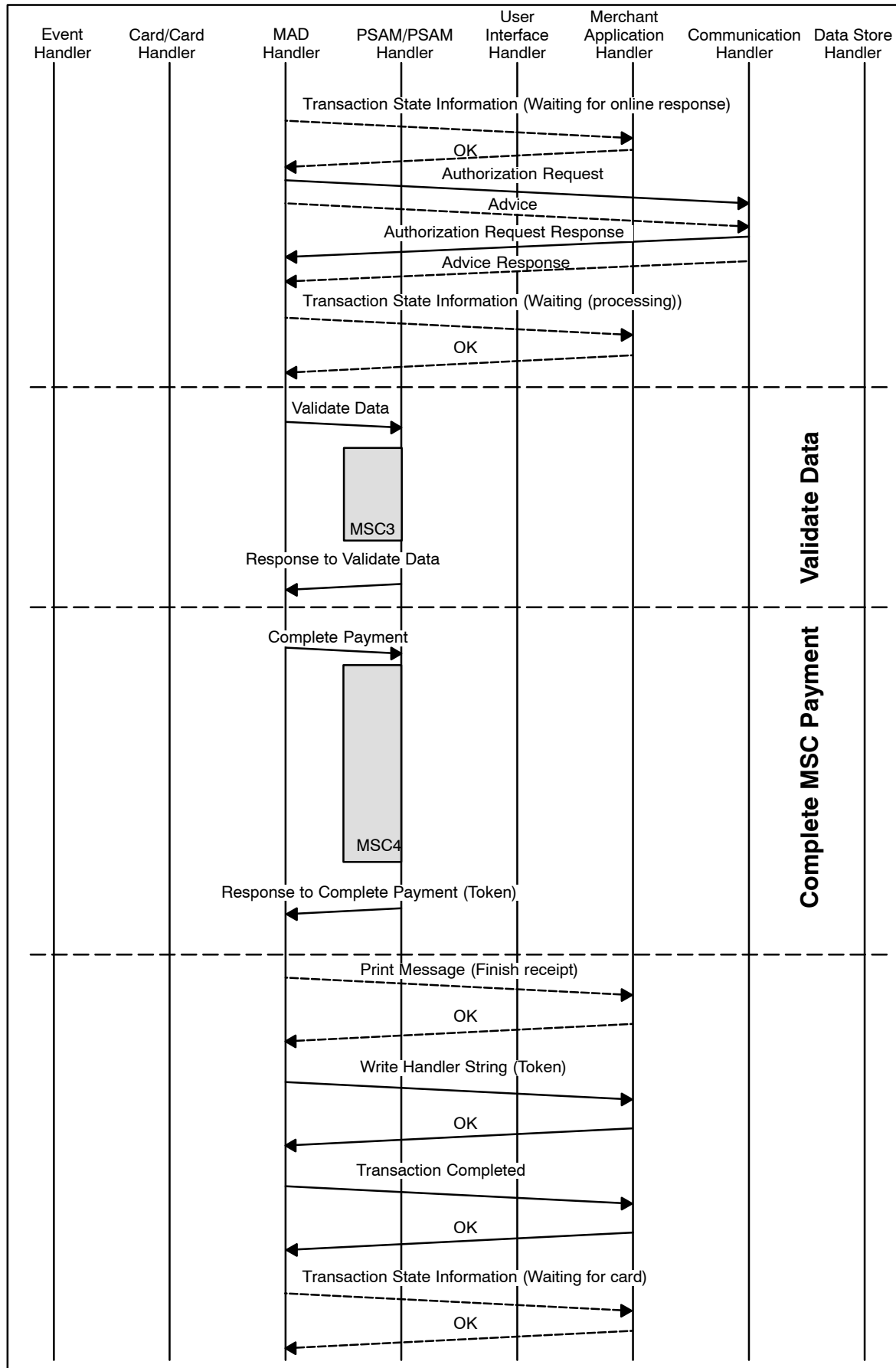


Figure 6.14 – MSC Transaction (Original Authorization – PIN) (concluded)



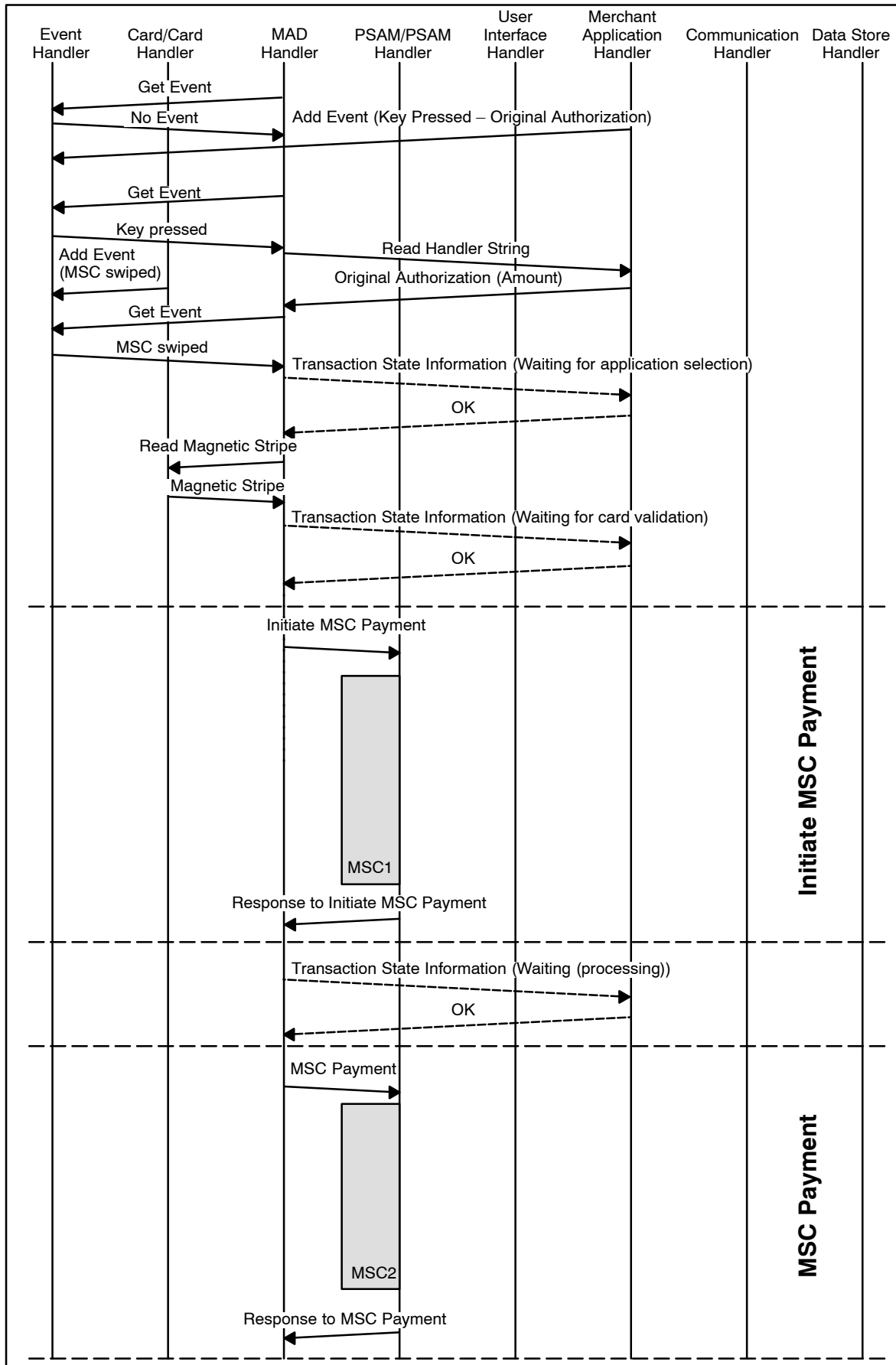


Figure 6.15 – MSC Transaction (Original Authorization – No CVM)

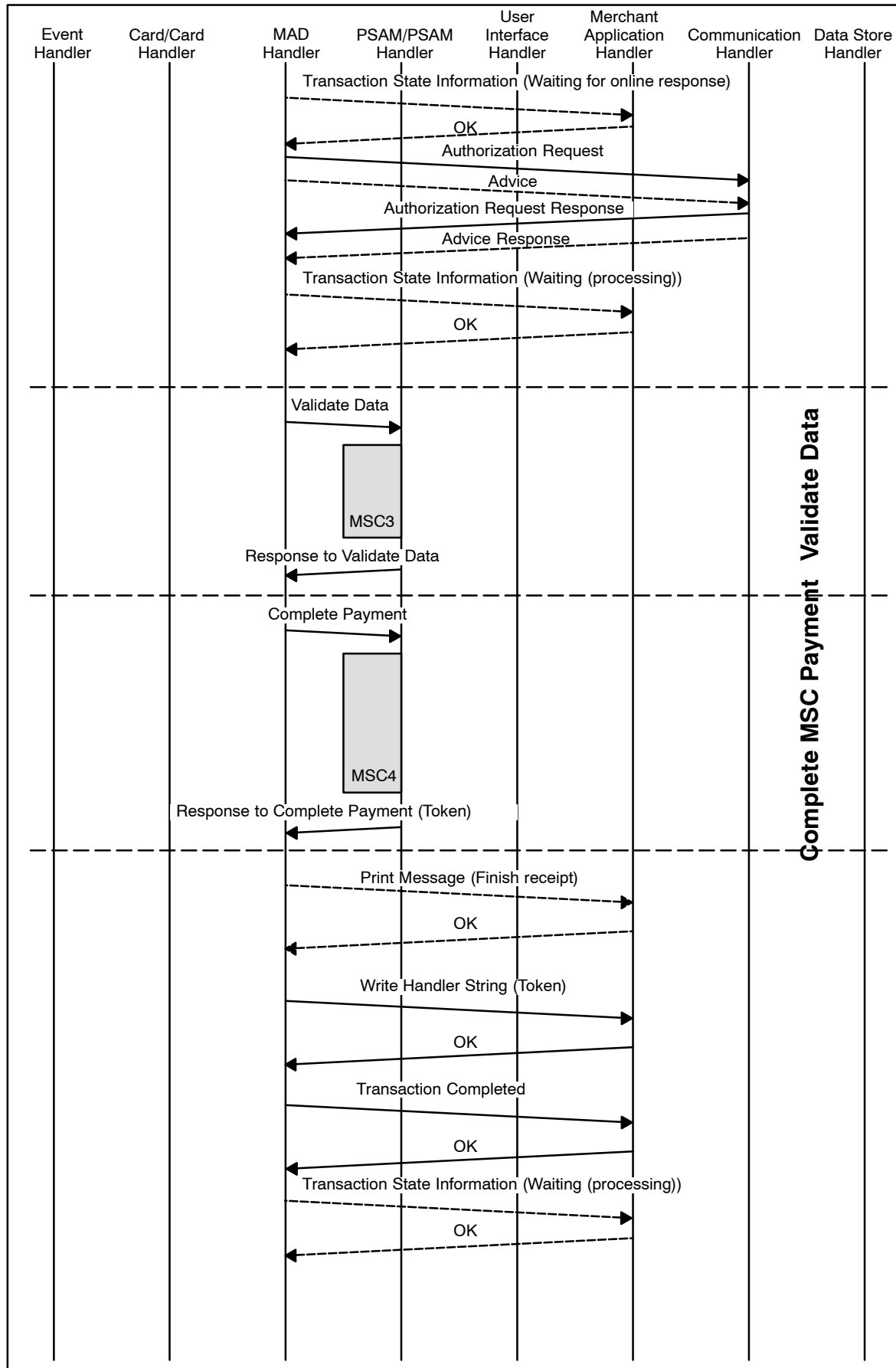


Figure 6.15 – MSC Transaction (Original Authorization – No CVM) (concluded)

## 6.13 Key Entered Card Transactions

### 6.13.1 Transaction Processing

The Merchant Application initiates the transaction by using the appropriate Business Call.

- 6.13.1.1 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.

- 6.13.1.2 A If the terminal supports backup logging of the transactions in the Merchant Application, the MAD–Handler shall indicate this in the data element “Info Level” which is part of 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.

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.

- 6.13.1.3 A For EMV cards where the IC is not readable, the fallback shall be the magnetic stripe. If the magnetic stripe neither is readable, a key entered transaction may be initiated if allowed.

Figure 6.16 to figure 6.18 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. 40: “TAPA, Application Architecture Specification”.

### 6.13.2 Initialization of the Key Entered Debit/Credit Payment Transaction

- 6.13.2.1 A The MAD–Handler shall frequently poll the Event Handler by sending a *Get Event* command to the Event Handler as defined in ref. 40: “TAPA, Application Architecture Specification”.

- 6.13.2.2 A If the response to the *Get Event* command indicates that a key (Business Call at the Merchant Application) has been pressed, the MAD–Handler shall send a *Read Handler String* command to the Merchant Application in order to get information of the type of Business Call.

- The way of entering the card data and initiating the Key Entered transaction is outside the scope of this specification.
- 6.13.2.3 A The key entered data (PAN || Expiry Date || CV-2) shall be stored in the Merchant Application and the PAN shall be transferred to the MAD-Handler.
- NOTE:** The PAN should e.g. be transferred by the *Read Handler String* command defined in requirement 6.13.2.3.
- 6.13.2.4 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 5.13.5 “MSC Application Selection”.
- 6.13.2.5 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.
- 6.13.2.6 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.

### 6.13.3 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.

- 6.13.3.1 A The *Initiate Key Entered Payment* command shall conform to the format defined in section 8.6.11.
- 6.13.3.2 A The data element “Card Data Source” shall be set to ‘02’ indicating Key Entered.
- 6.13.3.3 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 Attachment G, “Receipts”.
- 6.13.3.4 A The data element “TR” (Transaction Request) shall be coded according to the Business Call initiated.
- 6.13.3.5 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).
- 6.13.3.6 A The “Terminal Ident.” (Terminal Identification) shall be coded according to ref. 36: “EMV, version 4.1”.

- 6.13.3.7 A The data element “POS Entry Mode” shall be coded according to Attachment F, section F.9.5.
- 6.13.3.8 A The data element “TT” (Transaction Type) shall be coded according to Attachment F, section F.9.2. Only the 2 most significant digits are indicated in TT.
- 6.13.3.9 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
- 6.13.3.10 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).
- 6.13.3.11 A Counters shall be reported *only* when they have been incremented.
- 6.13.3.12 A The field “Statistics” shall be TLV coded. The tags and format for the different data elements are defined in Attachment F, section F.9.11.
- NOTE:** Please observe that the key entered data (PAN || Expiry Date || CV-2) will be obtained by the PSAM directly from the Merchant Application.

### Entering the Amount

For the Purchase/Refund 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.

- 6.13.3.13 A The length field LEN<sub>AMOUNTS</sub> shall indicate the appropriate length of all the amount related fields.
- 6.13.3.14 A In cases where cashback is allowed, this amount (Amount, Other) shall be indicated separately in the *Initiate Key Entered Payment* command.

It is for to the Terminal Supplier to engage a dialogue 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.

- 6.13.3.15 A For the Original Authorization transactions, the amount shall be present before the *Initiate Key Entered Payment* command is issued.

### Response

When the PSAM has responded to the *Initiate Key Entered Payment* command, the application control is returned over to the MAD-Handler.

The response to the *Initiate Key Entered Payment* command will conform to the format defined in section 8.6.11.

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 Key Entered Payment* command.

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.

The Application Status Words (ASW1-ASW2) will indicate the processing status of the *Initiate Key Entered Payment* command. The possible values of ASW1-ASW2 are defined in table 8.108 to table 8.119.

- 6.13.3.16 A If guidance of the merchant is enabled, the MAD-Handler shall send a *Transaction State Information* command (indicating “Processing”) to the Merchant Application.

## 6.13.4 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.

- 6.13.4.1 A The *Key Entered Payment* command shall conform to the format defined in section 8.6.12.

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.

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.
- 6.13.4.2 A The actual implementation of the Stop List shall not affect the value of the data element Stop List Status.
- 6.13.4.3 A Voice Authorization has priority to validation against a Stop List.
- 6.13.4.4 A An electronic Stop List has priority to validation against a manual Stop List.
- 6.13.4.5 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.
- 6.13.4.6 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 6.5.
- 6.13.4.7 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/Authorisation Code.
- 6.13.4.8 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.
- 6.13.4.9 B If the Merchant Application is configurable based upon a decision that Voice Authorization in general is never feasible, the decision of the actual configuration shall be made by the merchant.
- 6.13.4.10 A If the card does not appear on the Stop List and the Voice Authorization is rejected, the “Stop List Status” shall be set to ‘80’.
- 6.13.4.11 A When no Approval Code/Authorisation Code has been entered, the field “Approval Code” in the response to the *Check Stop List* command shall be filled with spaces.
- 6.13.4.12 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 *Key Entered Payment* command. The Batch Number will be part of the Financial Requests and Reversals created by the PSAM. See section 6.16.10 for more details concerning the Batch Number.

- 6.13.4.13 A If the MDOL1 (MAD-Handler Data Object List) given in the response to the *Initiate Key Entered Payment* command indicates that additional data is required, the MAD-Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists.

### 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 8.6.12.

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 *Key Entered Payment* command.

If the PSAM/terminal has determined that an online transaction is required, the PSAM will return a complete (including APACS header) Financial Request or Authorization Request according to Attachment F.

- 6.13.4.14 A If an online transaction is requested, the MAD-Handler shall initiate a communication session according to ref. 40: “TAPA, Application Architecture Specification”.

- 6.13.4.15 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 online 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.

- 6.13.4.16 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.



## 6.13.5 Validate Data

### Command

By issuing a *Validate Data* command to the PSAM, application control is handed over from the MAD–Handler to the PSAM.

**NOTE:** The *Validate Data* command may consist of one or two segments depending of the amount of data.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command should be utilized.

- |          |   |  |
|----------|---|--|
| 6.13.5.1 | A | The <i>Validate Data</i> command shall conform to the format defined in section 8.6.4 or 8.6.5.  |
| 6.13.5.2 | A | If the MDOL2 (MAD–Handler Data Object List) given in the response to the <i>Key Entered Payment</i> command indicates that additional data is required, the MAD–Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists. |
| 6.13.5.3 | 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 Attachment F.  |
| 6.13.5.4 | A | If the terminal has <i>not</i> been online, the length field LEN <sub>HR</sub> shall be set to zero.   |

### Response

When the PSAM has responded to the *Validate Data* command, the application control is returned to the MAD–Handler.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command response should be utilized. For more details concerning the data elements returned and their usage when printing receipts, see Attachment G, “Receipts”.

The response to the *Validate Data* or *Validate Data 2* command will conform to the format defined in section 8.6.4 or 8.6.5.

The Action Code (AC or AC<sub>PRINT</sub>) will inform the MAD–Handler of status of the host response in case of online transaction and the PSAM status in case of an offline transaction.

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.

- |          |   |   |
|----------|---|---|
| 6.13.5.5 | A | If the “Host Request” data element is present in the response to the <i>Validate Data</i> or <i>Validate Data 2</i> command, the MAD–Handler shall send the host request and continue the processing from the state where the response to <i>Key Entered Payment</i> command is just received and continue as normal. |
|----------|---|---|

### 6.13.6 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.

- 6.13.6.1 A The *Complete Key Entered Payment* command shall conform to the format defined in section 8.6.13.
- 6.13.6.2 A The data element “Transaction Status” shall be coded according to the coding defined for this data element.
- 6.13.6.3 A In case of a signature based transaction if 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 Key Entered Payment* command, the application control is handed back to the MAD-Handler.

The response to the *Complete Key Entered Payment* command will conform to the format defined in section 8.6.13.

If the transaction is an Original Authorization, then the response to the *Complete Key Entered Payment* command will contain a Token as defined in section 6.5.

**NOTE:** Supplementary Authorization is described in section 6.14, “Token Based Transactions”.

- 6.13.6.4 A The MAD-Handler shall convey the Token to Merchant Application by utilizing a *Write Handler String* command to Merchant Application Handler in case of an Original Authorization transaction.
- 6.13.6.5 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.
- 6.13.6.6 A The cardholder shall be informed of the result of the transaction according to the requirement defined in section 5.6.4, “Sub-handler, Cardholder Display” and chapter 10, “Design Requirements”.

- 6.13.6.7 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

The layout of the receipts and the information printed depends on the transaction result and the type of CVM used as stated in Attachment G, “Receipts”.

- 6.13.6.8 A The receipts shall include the parameters identifying the merchant, the terminal and the card as defined in Attachment G, “Receipts”.
- 6.13.6.9 A The MAD–Handler shall for all transactions initiate printing of a receipt as defined in Attachment G.
- 6.13.6.10 C Printing of the receipt should be initiated in parallel with the PSAM dialogue in order to speed up the transaction.
- 6.13.6.11 A The PAN shall be part of the receipt printed with some of the digits truncated as stated in Attachment G, “Receipts”.
- 6.13.6.12 A The STAN to be printed on the receipt shall be taken from the response to the *Initiate Key Entered Payment* command.
- 6.13.6.13 A If a response to either an Authorization Request or a Financial Request is received from the host, the Card Name to be printed on the receipt shall be taken from this response. If no response is received, the Card Name to be printed on the receipt shall be taken from the response to the *Initiate Key Entered Payment* command.
- 6.13.6.14 A If the transaction is signature based and successful, the MAD–Handler shall initiate the final printing of the receipt in order to make it possible for the cardholder to sign a copy the receipt.
- 6.13.6.15 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.
- 6.13.6.16 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.

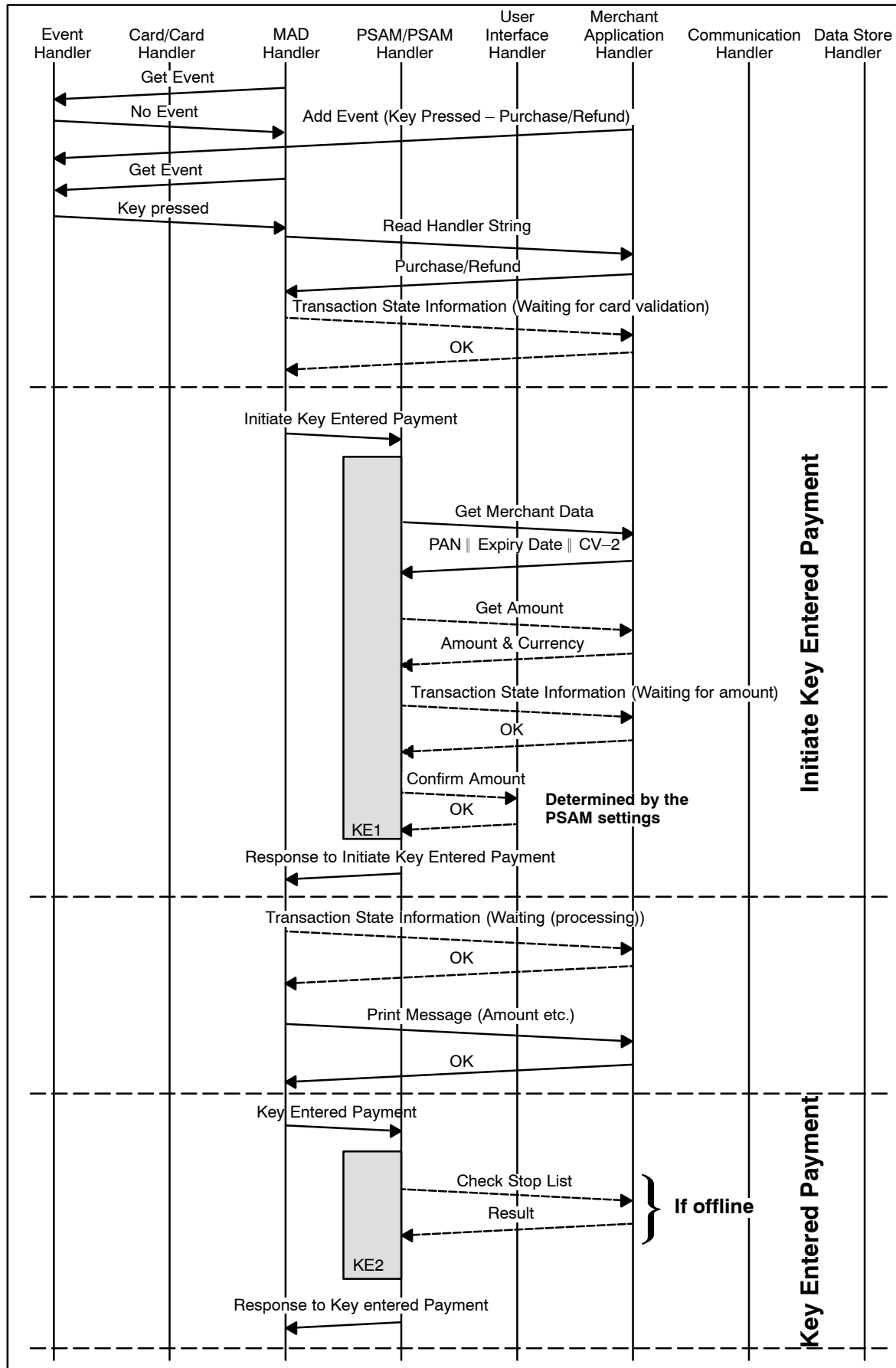


Figure 6.16 – Key Entered Transaction (Purchase/Refund – Signature)

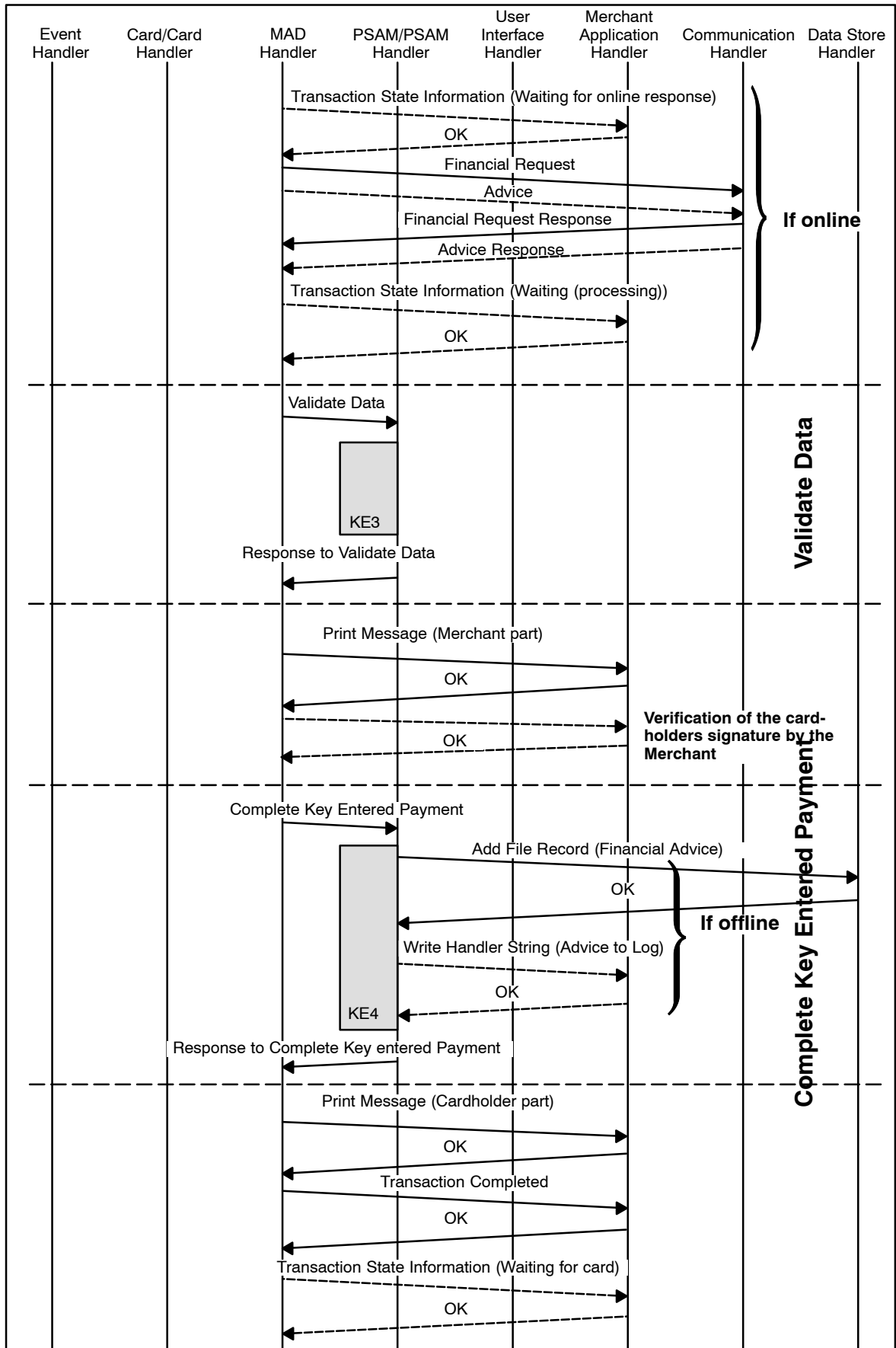


Figure 6.16 – Key Entered Transaction (Purchase/Refund – Signature) (concluded)

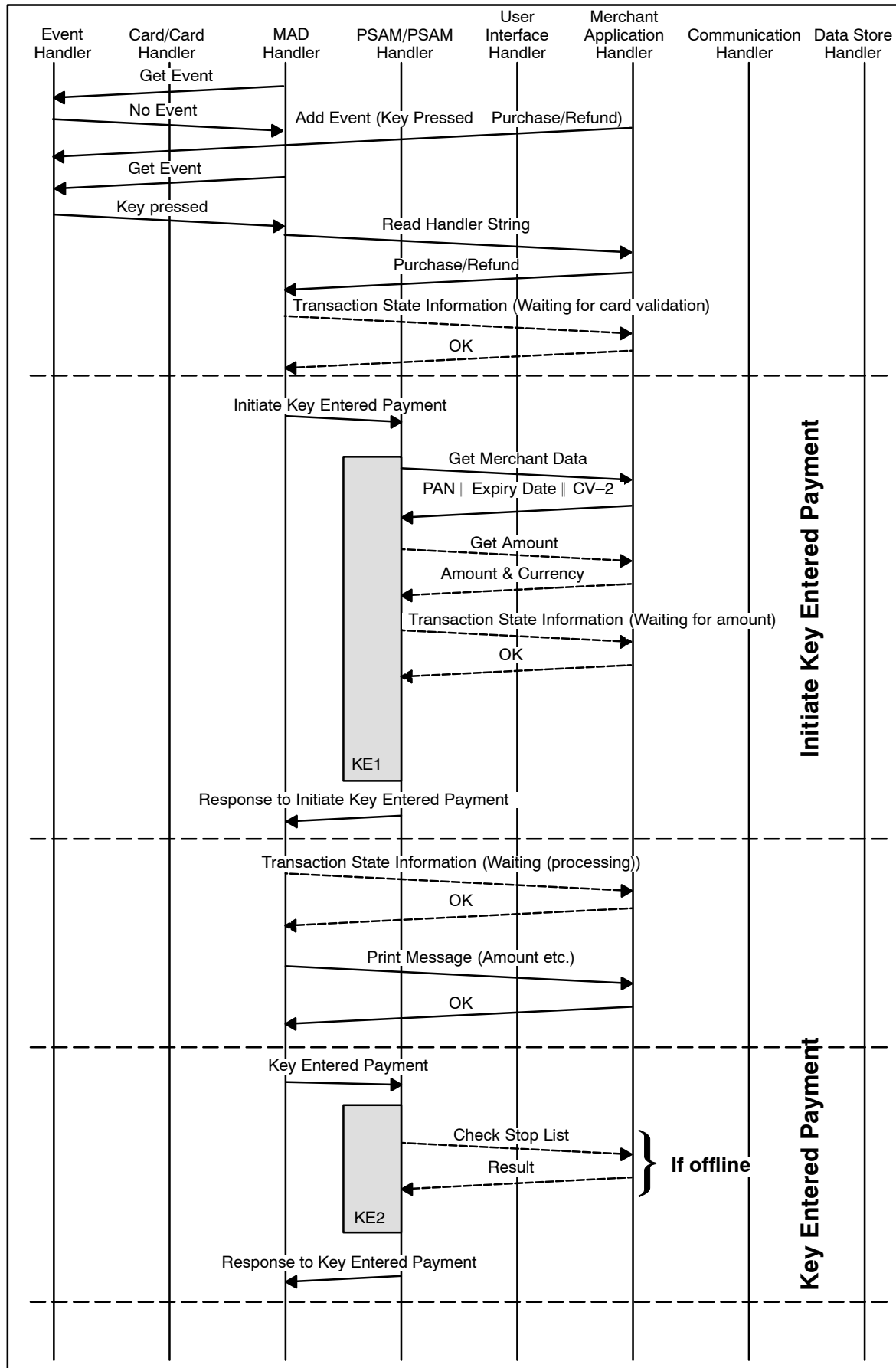


Figure 6.17 – Key Entered Transaction (Purchase/Refund – No CVM)

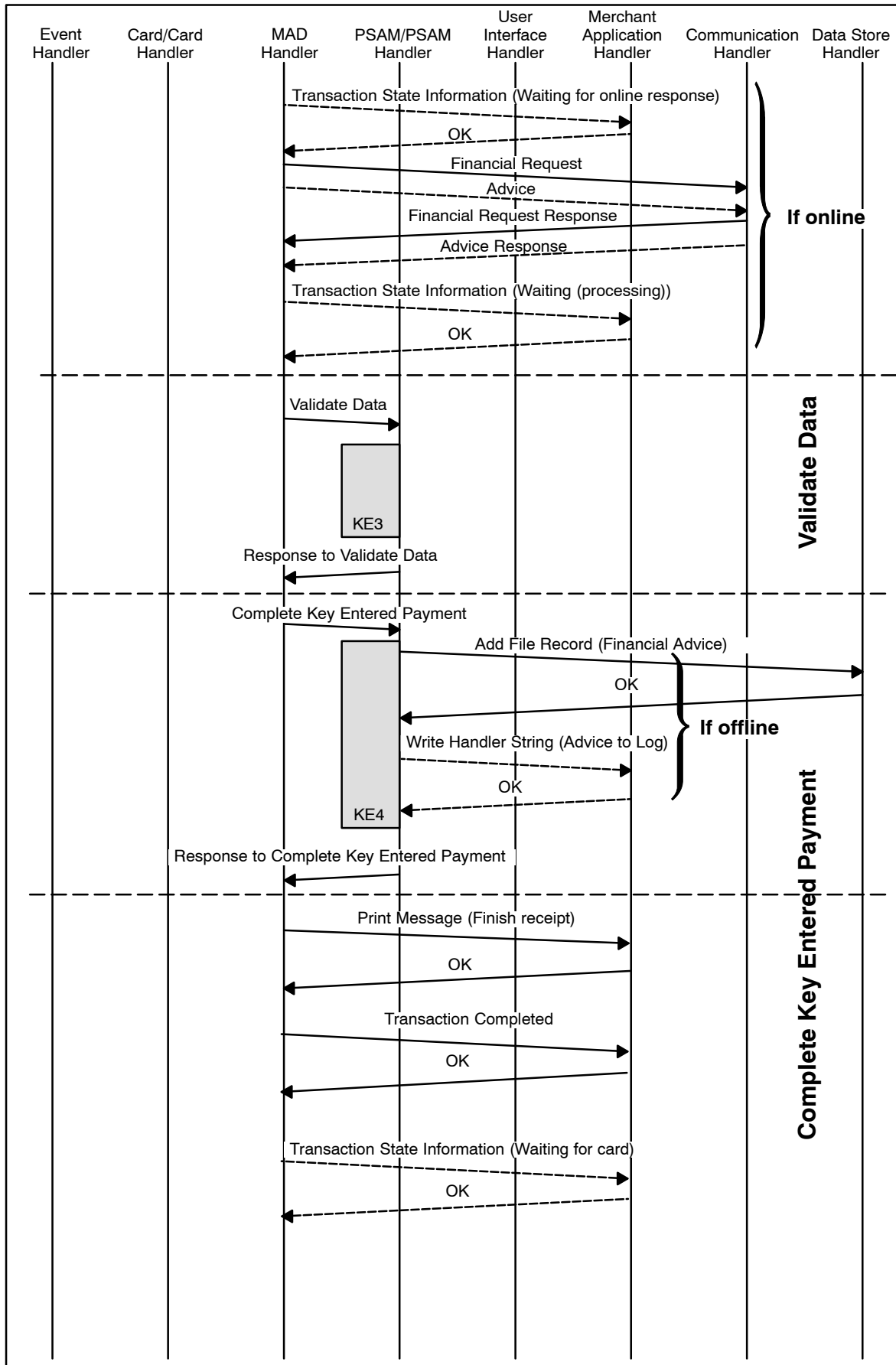


Figure 6.17 – Key Entered Transaction (Purchase – No CVM) (concluded)

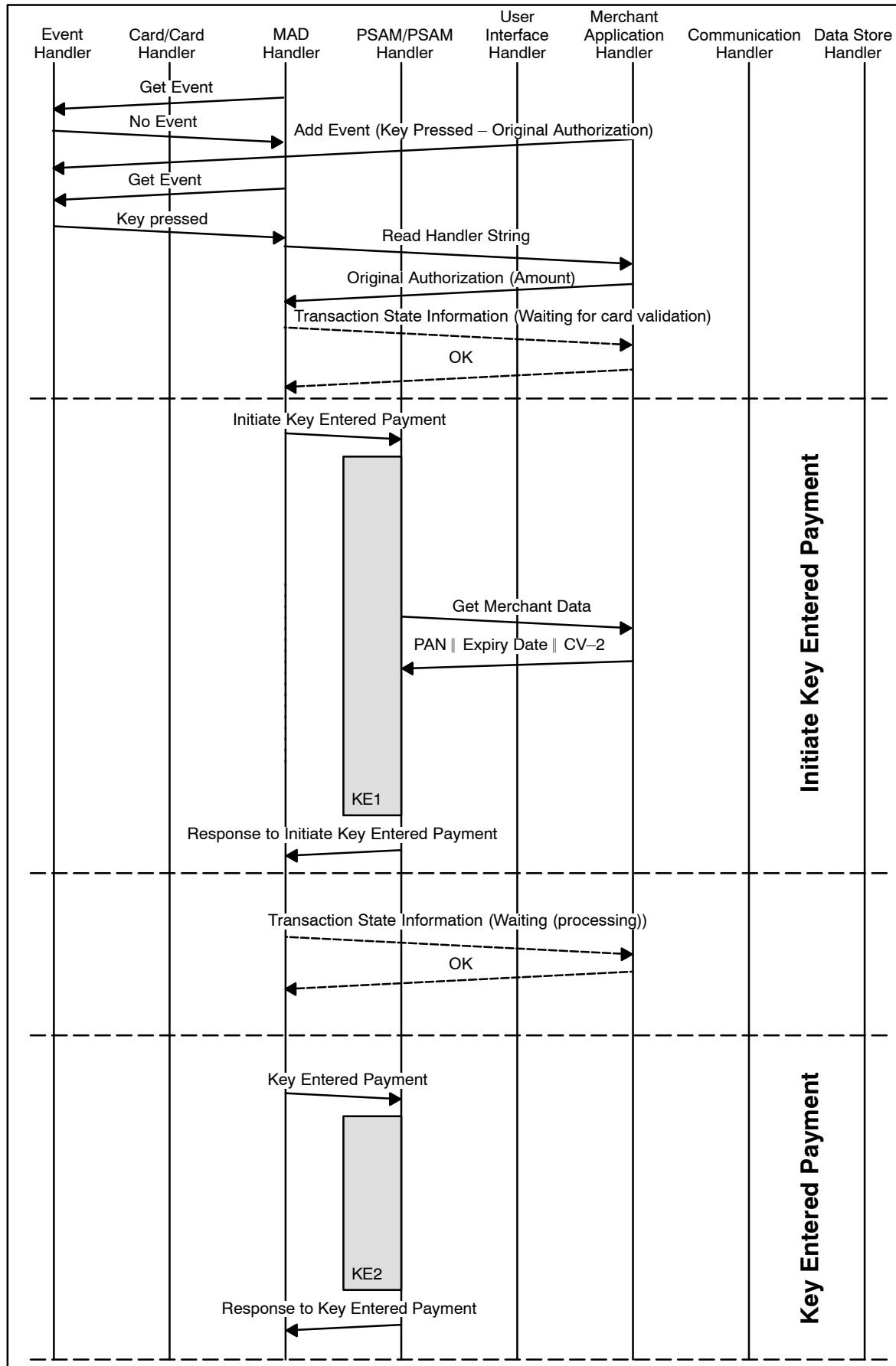


Figure 6.18 – Key Entered Transaction (Original Authorization – No CVM)



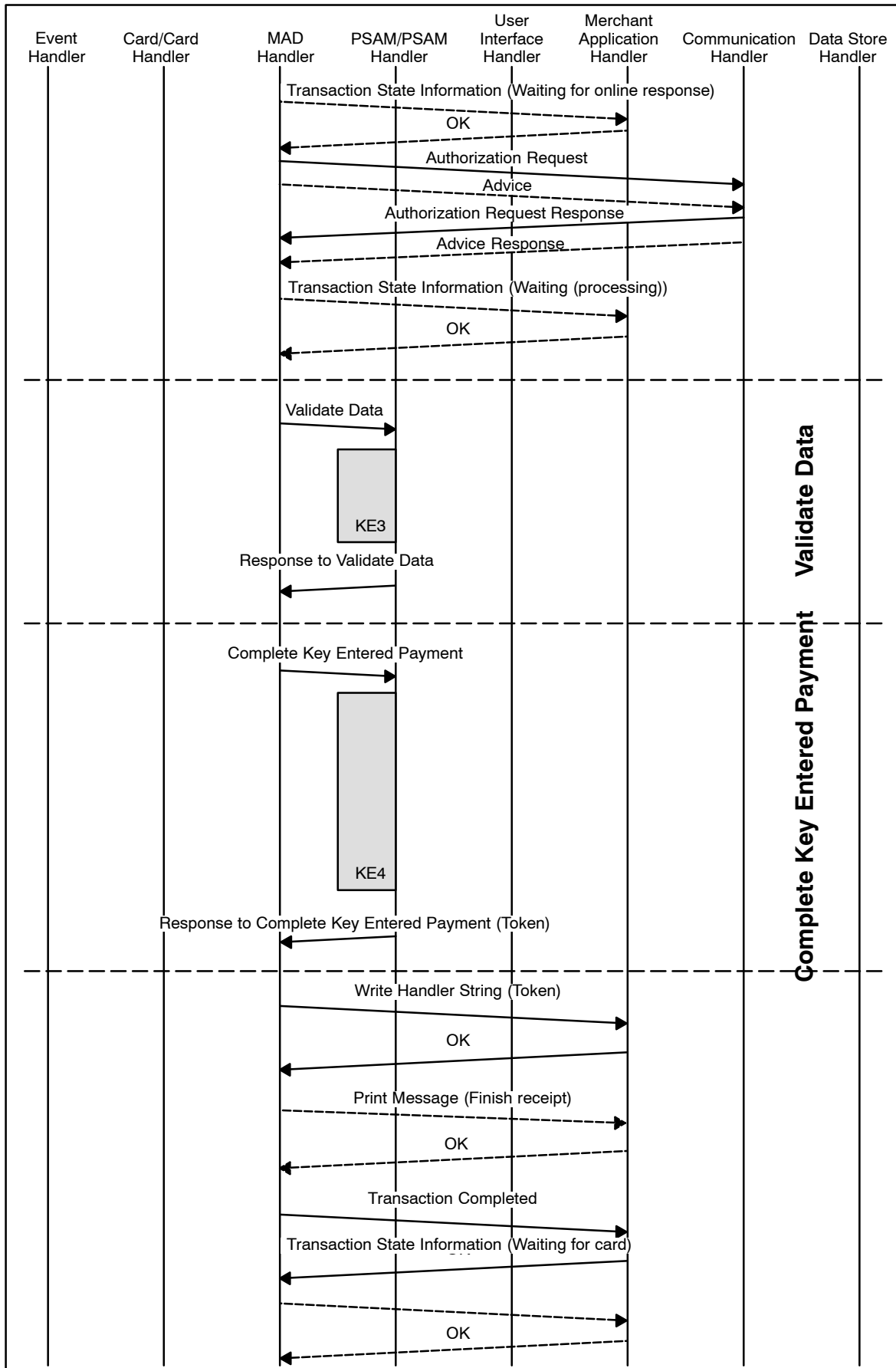


Figure 6.18 – Key Entered Transaction (Original Authorization – No CVM) (concluded)

## 6.14 Token based Transactions

### 6.14.1 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 Authorization results in Token as output, this transaction is not part of the Token based transactions. See section 6.10 & 6.12 for further details.

- 6.14.1.1      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.

- 6.14.1.2      A      If the terminal supports backup logging of the transactions in the Merchant Application, the MAD-Handler shall indicate this in the data element “Info Level” which is part of 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.

Figures 6.19 to 6.22 provides examples of typical message flows for successful Token Based transactions. For a description of the handlers depicted in the figures, refer to ref. 40: “TAPA, Application Architecture Specification”.

### 6.14.2 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.

- 6.14.2.1 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.
- 6.14.2.2 A As soon as the MAD–Handler has been informed that a Token is available, the MAD–Handler shall perform application selection based on the two data elements from 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. The application selection will then be based on either the Application Identifier or the PAN–prefix, using the principles defined in respectively section 5.13.5 “ICC Application Selection” and section 5.13.4 “MSC Application Selection”.
- 6.14.2.3 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”, the application has been selected.

### 6.14.3 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.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 2, the *Initiate Token Based Payment 2* command should be utilized.

- 6.14.3.1 A The *Initiate Token Based Payment* command shall conform to the format defined in section 8.6.14.
- 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.
- 6.14.3.2 A The data element “Card Data Source” shall be set to ‘03’ indicating Token Based.
- 6.14.3.3 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 Attachment G, “Receipts”.

- 6.14.3.4 A The data element “TR” (Transaction Request) shall be coded according to the Business Call initiated.
- 6.14.3.5 A The Merchant Initiative (“MI”) shall be set to ‘00’ indicating that the merchant does not force either the transaction online/off-line or force a specific CVM.
- 6.14.3.6 A The “Terminal Ident.” (Terminal Identification) shall be coded according to ref. 36: “EMV, version 4.1”.
- 6.14.3.7 A The data element “TT” (Transaction Type) shall be coded according to Attachment F, section F.9.2. Only the 2 most significant digits are indicated in TT.
- 6.14.3.8 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
- 6.14.3.9 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).
- 6.14.3.10 A Counters shall be reported *only* when they have been incremented.
- 6.14.3.11 A The field “Statistics” shall be TLV coded. The tags and format for the different data elements are defined in Attachment F, section F.9.11.

### Entering the Amount

- 6.14.3.12 A For all Token Based transactions, the amount shall be present before the *Initiate Token Based Payment* command is issued.
- 6.14.3.13 A The length field LEN<sub>AMOUNTS</sub> shall indicate the appropriate length of all the amount related fields.
- 6.14.3.14 A Cashback shall not be allowed, thus the field Amount, Other shall either be set to zero or omitted in the *Initiate Token Based Payment* command.

**NOTE:** The host or PSAM may decline a transaction if the currency is not supported.

It is up to the Terminal Supplier to engage in a dialogue with the merchant to determine the currencies to support. The way of se-

lecting the different currencies by the merchant is out of scope of this specification.

### Account Type

- 6.14.3.15 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 9.2.1 on page 9–2 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 8.6.14.

The Merchant Number (“ME<sub>NUMBER</sub>”), 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<sub>NUMBER</sub> is accepted/valid in the present store.

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 Token Based Payment* command.

- 6.14.3.16 A The STAN to be printed on the receipt shall be taken from the response to the *Initiate Token Based Payment* command.

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.

The Application Status Words (ASW1–ASW2) will indicate the processing status of the *Initiate Token Based Payment* command. The possible values of ASW1–ASW2 are defined in table 8.108 to table 8.119.

- 6.14.3.17 A If guidance of the merchant is enabled, the MAD–Handler shall send a *Transaction State Information* command (indicating “Processing”) to the Merchant Application.

## 6.14.4 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.

- 6.14.4.1 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 *Token Based Payment* command. The Batch Number will be part of the Financial Advices and Reversals created by the PSAM. See section 6.16.10 for more details concerning the Batch Number.
- 6.14.4.2 A If the MDOL1 (MAD–Handler Data Object List) given in the response to the *Initiate Token Based Payment* command indicates that additional data is required, the MAD–Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists.

### 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 8.6.16.

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 *Token Based Payment* command.

If the PSAM has determined that an online transaction is required, the PSAM will return a complete (inclusive APACS header) Authorization Request according to Attachment F.

Supplementary Authorization transactions will always require an online connection to the acquirer host. The remaining types of Token Based transactions are performed offline.

- 6.14.4.3 A If an online transaction is requested, the MAD–Handler shall initiate a communication session according to ref. 40: “TAPA, Application Architecture Specification”.
- 6.14.4.4 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 online 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.
- 6.14.4.5 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.

## 6.14.5 Validate Data

### Command

By issuing a *Validate Data* command to the PSAM, application control is handed over from the MAD–Handler to the PSAM.

**NOTE:** The *Validate Data* command may consist of one or two segments depending of the amount of data.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command should be utilized.

- 6.14.5.1 A The *Validate Data* or *Validate Data 2* command shall conform to the format defined in section 8.6.4 or 8.6.5.
- 6.14.5.2 A If the MDOL2 (MAD–Handler Data Object List) given in the response to the *Token Based Payment* command indicates that additional data is required, the MAD–Handler shall provide the data using the rules defined in ref. 36: “EMV, version 4.1” for Data Object Lists.
- 6.14.5.3 A When the terminal has been online, the MAD–Handler shall provide the message response received from the host (without the APACS header) as defined in Attachment F.

### Response

When the PSAM has responded to the *Validate Data* command, the application control is returned to the MAD–Handler.

**NOTE:** For terminals where both terminal and PSAM support Service Pack No. 1, the *Validate Data 2* command response should be utilized. For more details concerning the data elements returned and their usage when printing receipts, see Attachment G, “Receipts”.

The response to the *Validate Data* or *Validate Data 2* command will conform to the format defined in section 8.6.4 or 8.6.5.

The Action Code (AC or AC<sub>PRINT</sub>) will inform the MAD–Handler of status of the host response.

## 6.14.6 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.

- 6.14.6.1 A The *Complete Token Based Payment* command shall conform to the format defined in section 8.6.17.
- 6.14.6.2 A The data element “Transaction Status” shall be coded according to the coding defined for this data element.
- 6.14.6.3 A In case of a signature based transaction if 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 Token Based Payment* command, the application control is handed back to the MAD-Handler.

The response to the *Complete Token Based Payment* command will conform to the format defined in section 8.6.17.

If the transaction is an Supplementary Authorization, then the response to the *Complete Token Based Payment* command will contain a Token as defined in section 6.5.

- 6.14.6.4 A The MAD-Handler shall convey the Token to Merchant Application by utilizing a *Write Handler String* command to Merchant Application Handler in case of an Supplementary Authorization transaction.
- 6.14.6.5 A The cardholder shall be informed of the result of the transaction according to the requirement defined in section 5.6.4, “Sub-handler, Cardholder Display” and chapter 10, “Design Requirements”.

**NOTE:** Requirement 6.14.6.5 is only relevant if the Cardholder is present.

- 6.14.6.6 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

- 6.14.6.7 A The receipts shall include the parameters identifying the merchant, the terminal and the card as defined in Attachment G, “Receipts”.
- 6.14.6.8 A The PAN shall be part of the receipt printed with some of the digits truncated as stated in Attachment G, “Receipts”.



- 6.14.6.9 A If a response to either an Authorization Request or a Financial Request is received from the host, the Card Name to be printed on the receipt shall be taken from this response. If no response is received, the Card Name to be printed on the receipt shall be taken from the response to the *Initiate EMV Payment* command.
- 6.14.6.10 A If the transaction is signature based and successful, the MAD–Handler shall initiate the final printing of the receipt in order to make it possible for the cardholder to sign a copy the receipt.
- 6.14.6.11 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.
- 6.14.6.12 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.

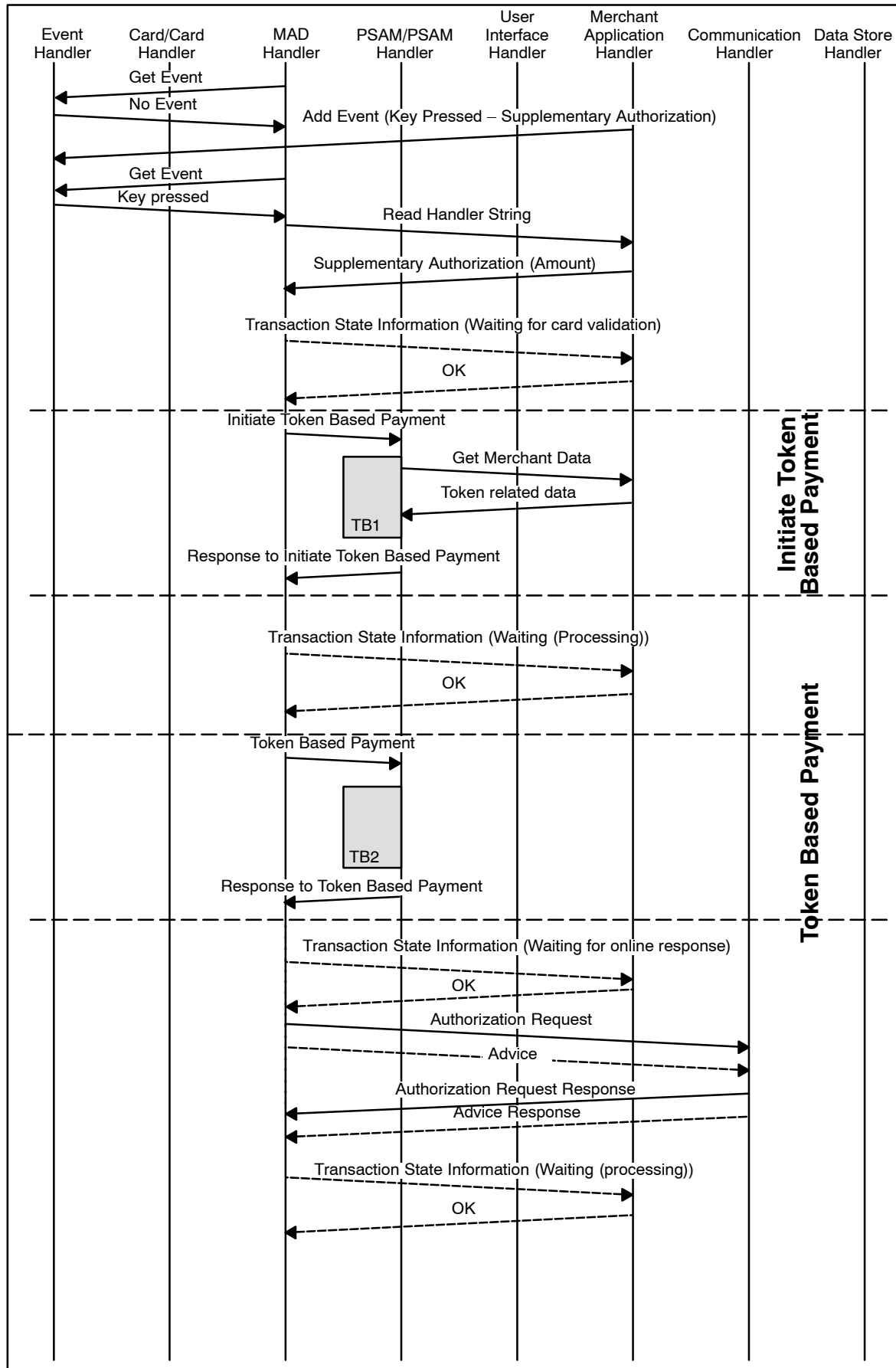


Figure 6.19 – Token Based Transaction (Supplementary Authorization – No CVM)

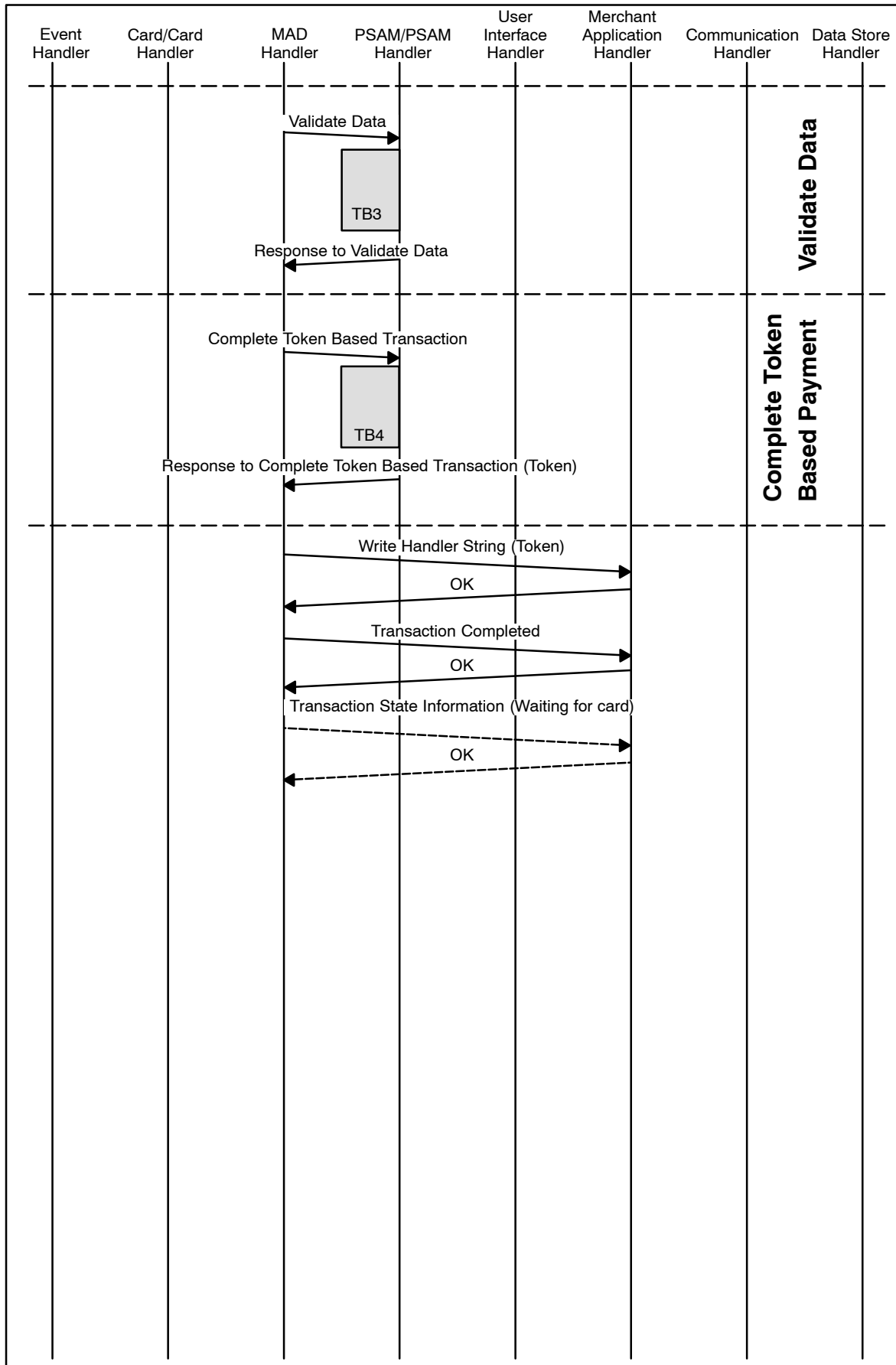


Figure 6.19 – Token Based Transaction (Suppl. Authorization – No CVM) (concluded)

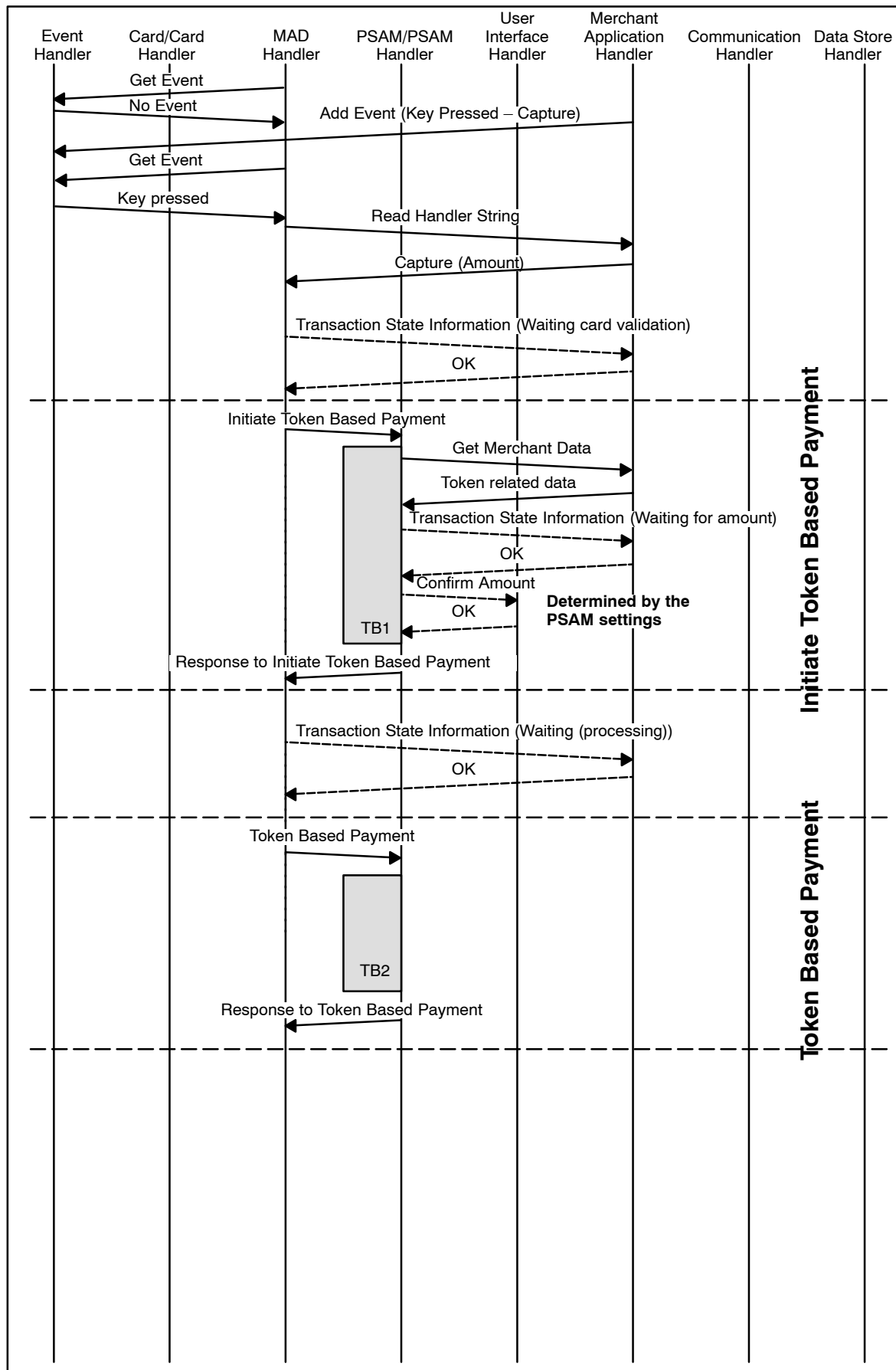


Figure 6.20 – Token Based Transaction (Capture – Signature)

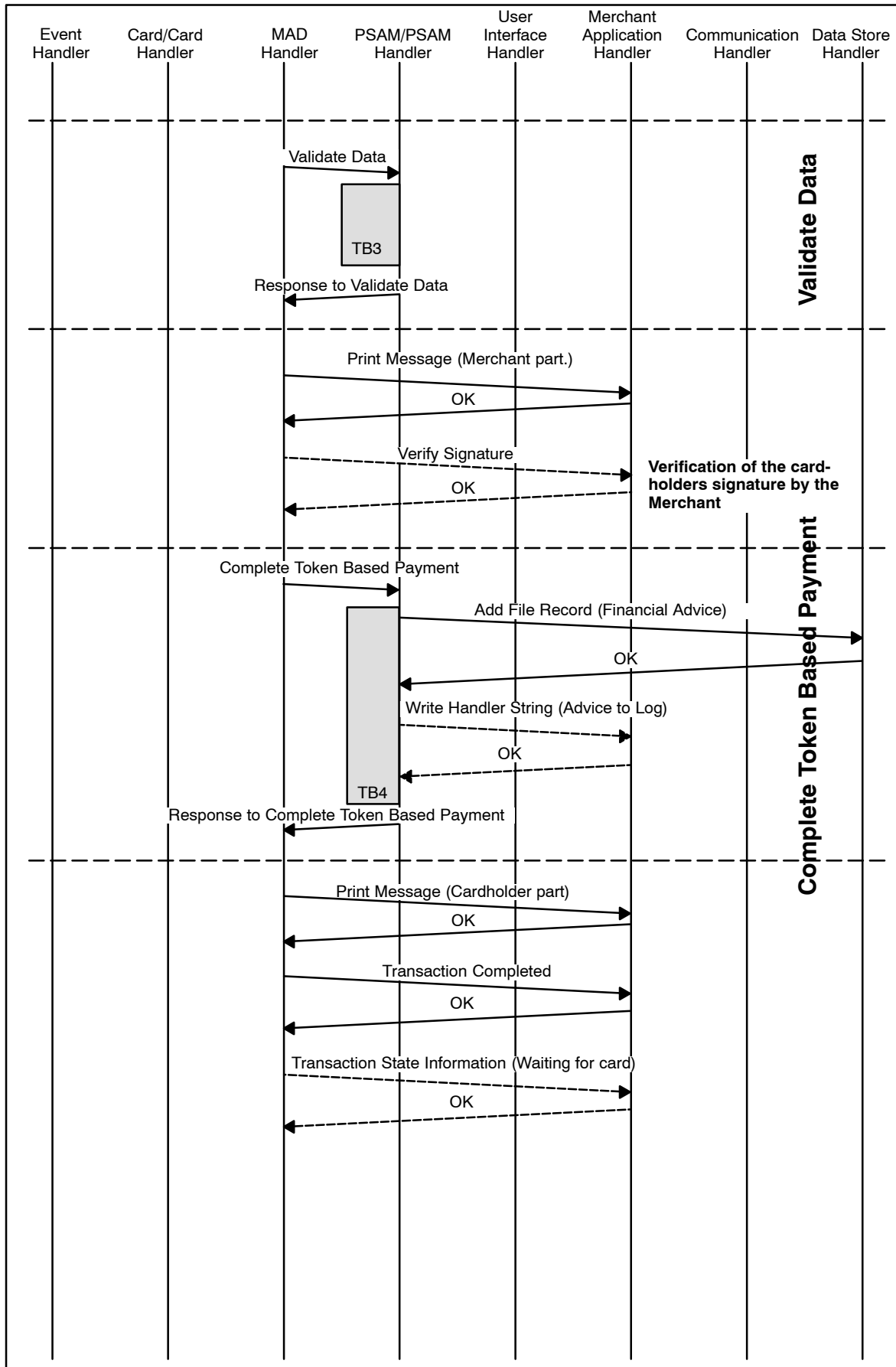


Figure 6.20 – Token Based Transaction (Capture – Signature) (concluded)

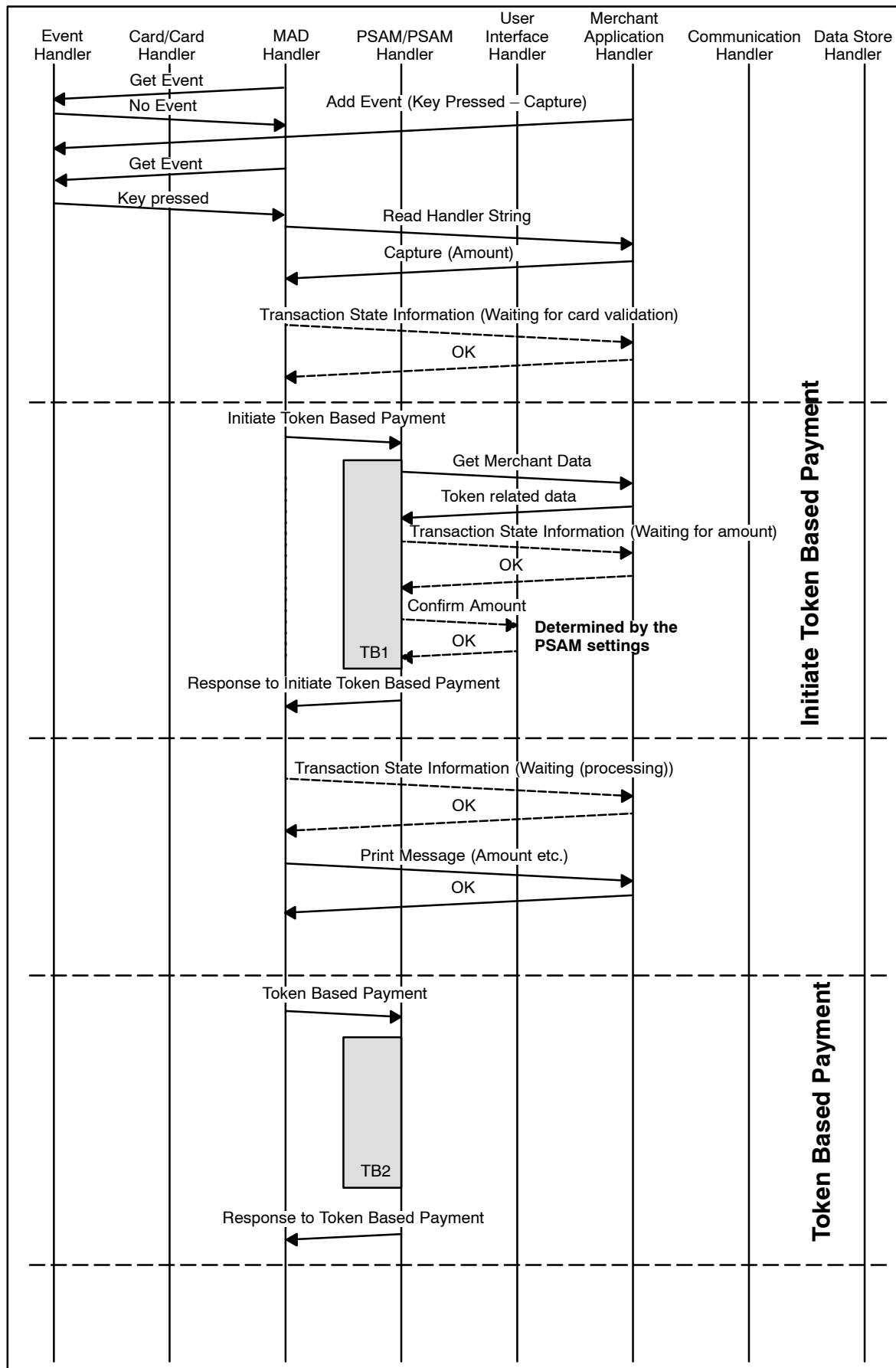


Figure 6.21 – Token Based Transaction (Capture – No CVM)

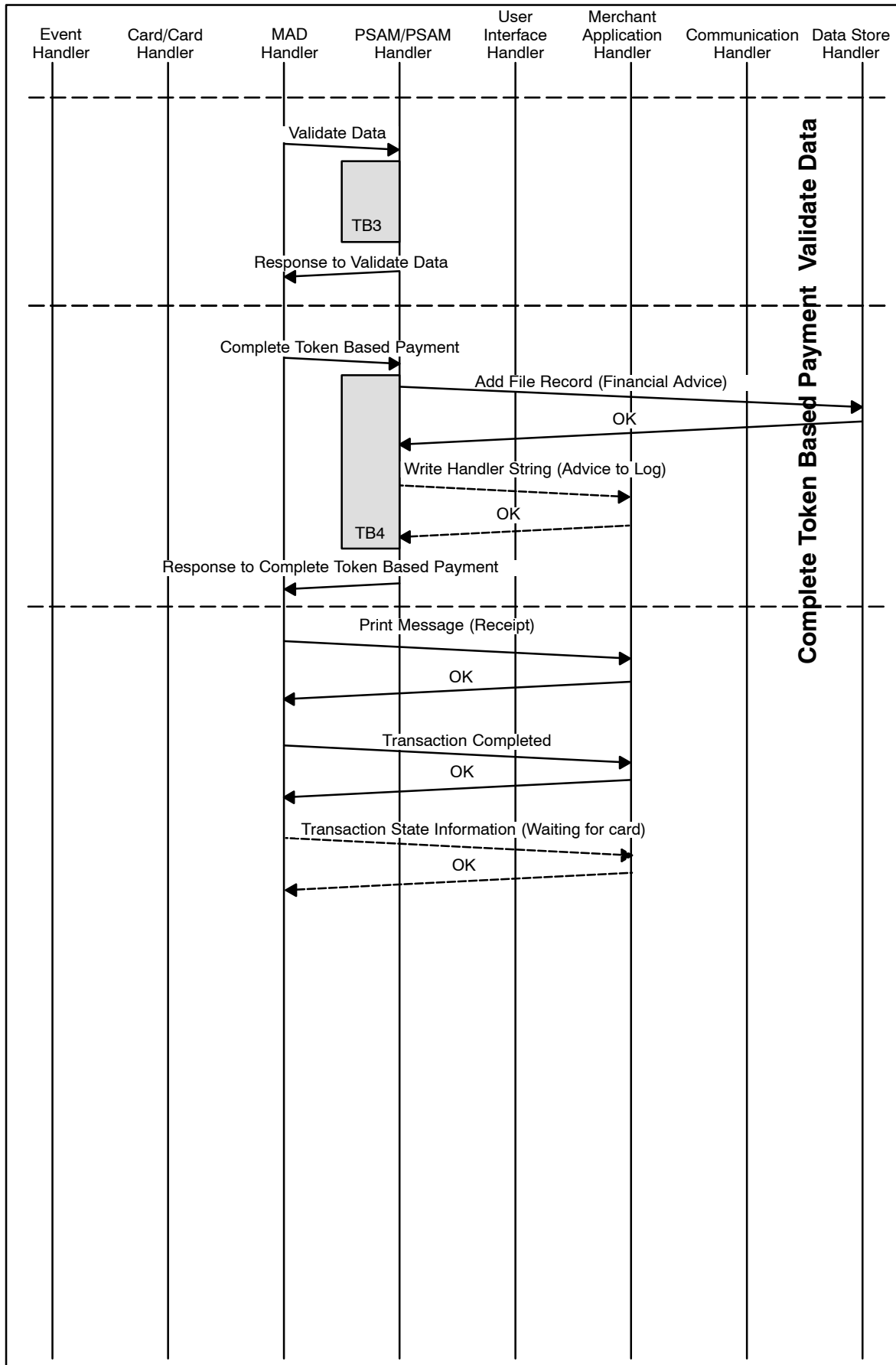


Figure 6.21 – Token Based Transaction (Capture – No CVM) (concluded)

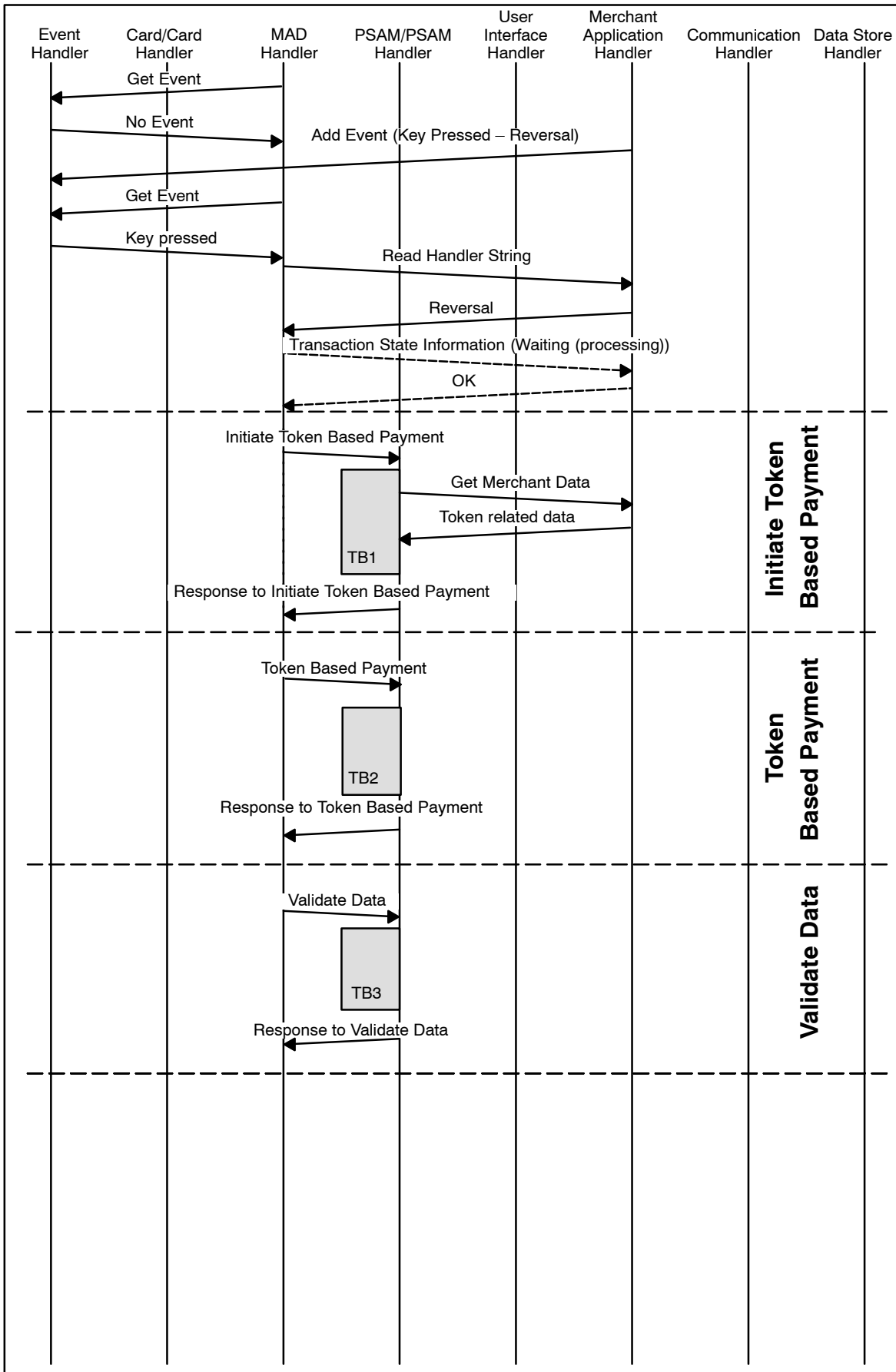


Figure 6.22 – Token Based Transaction (Reversal (Authorization) – No CVM)



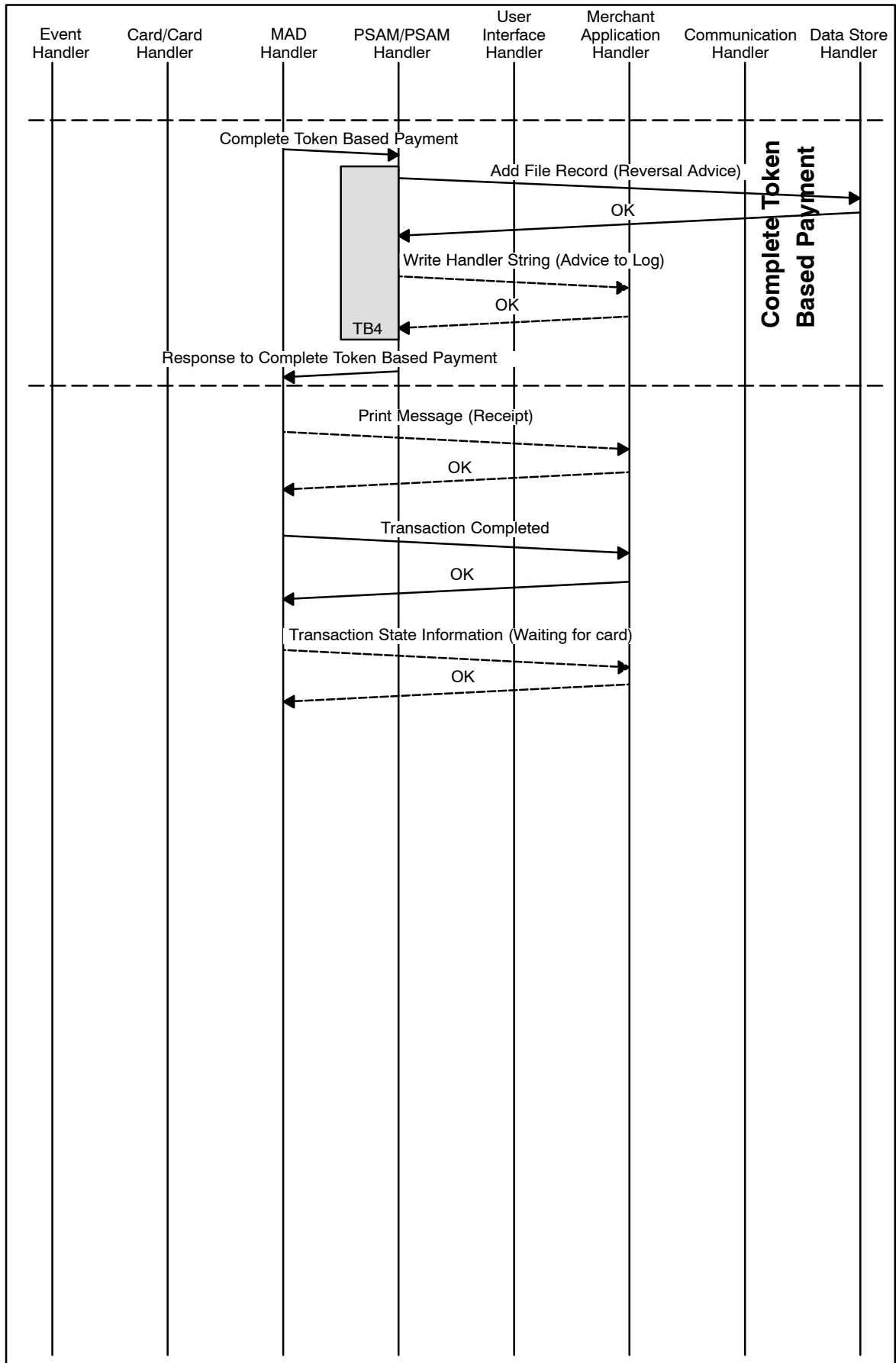


Figure 6.22 – Token Based Transaction (Reversal (Authorization) – No CVM) (concluded)

## 6.15 Addendum Records

### 6.15.1 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 Attachment F, section F.9.20.

### 6.15.2 Handling of Addendum Records

#### Pre-conditions

Addendum Records can *only* be attached to successful Captures.

- 6.15.2.1 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

- 6.15.2.2 A The terminal shall issue an *Add Addendum Record* command to the PSAM immediately after the Capture is performed.

**NOTE:** It is a business requirement from the card issuers that the Addendum Record shall 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.

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 Attachment F, section F.8.7).

**NOTE:** The *Add Addendum Record* command will cause the System Trace Audit Number (STAN) to be incremented.

- 6.15.2.3 A An *Add Addendum Record* command shall always be issued to the same PSAM where the previous financial transaction was performed.
- 6.15.2.4 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.
- 6.15.2.5 A An additional *Add Addendum Record* command shall succeed the *Complete Payment* command.

Table 6.15 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 6.15 – Source of the Data Elements Included in the *Add Addendum Record* Command

Data Elements	Source
Addendum Status	Terminal/Merchant Application
LEN <sub>PAN</sub>	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 Attachment F, section F.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 <sub>ADD</sub>	Terminal/Merchant Application
Addendum Record	Terminal/Merchant Application

### Complete Payment Command

- 6.15.2.6 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.
- 6.15.2.7 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 to be logged!).

An example of the command flow between different handlers is depicted in figure 6.23.

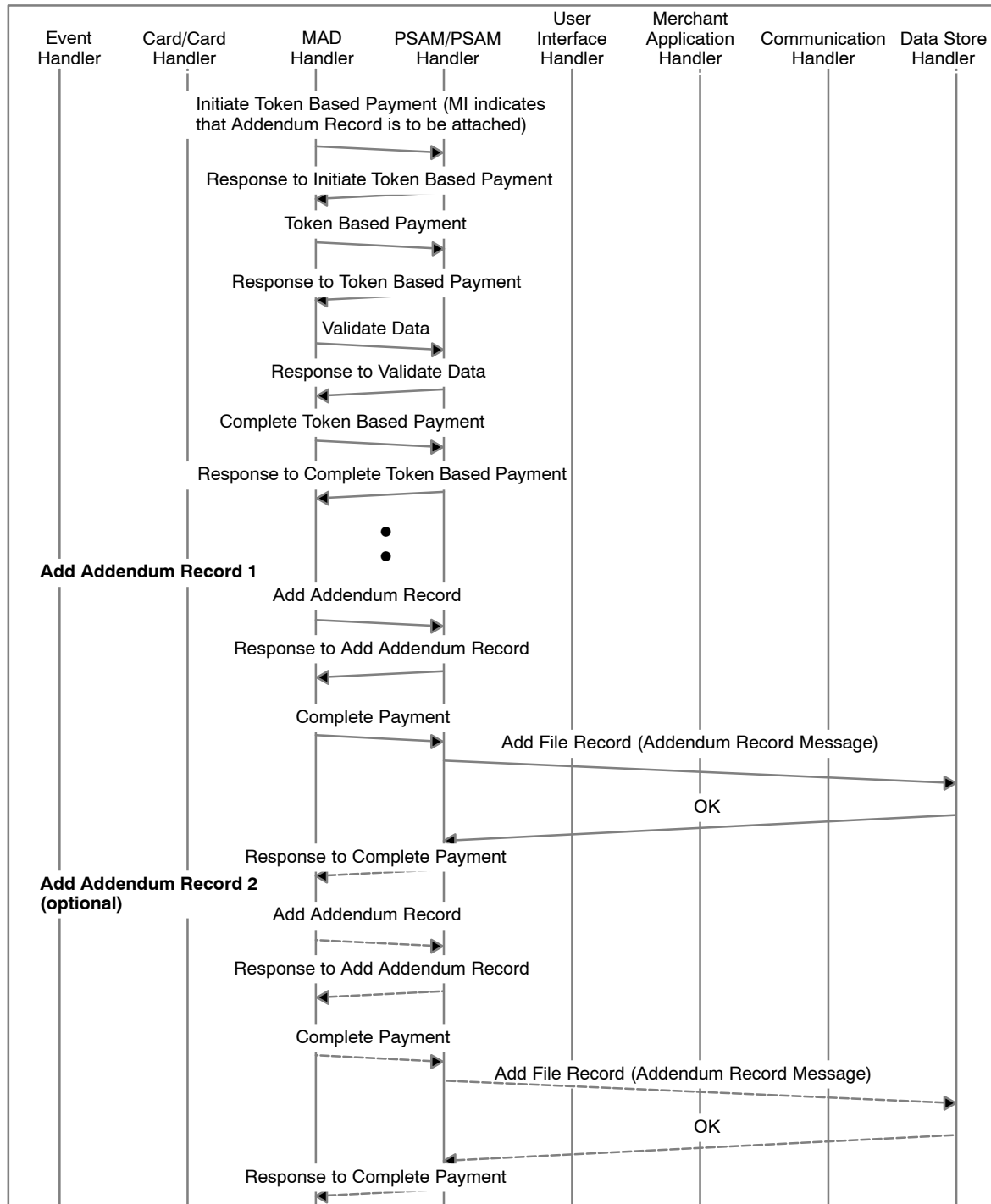


Figure 6.23 – Example of Addendum Record Command Flow (Capture)

## 6.16 Administrative Transactions and Processes

### 6.16.1 Introduction

Administrative routines are initiated by either the merchant or automatically for POS terminals. For a CAT 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 6.16.

Table 6.16 – 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 or the Merchant Application in order to empty the Data Store.

To avoid a accumulation of advices in the Data Store, two additional procedures are specified:

- Advice Enclosing,
- Advice Forwarding

- 6.16.1.1 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.

### 6.16.2 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.

6.16.2.1 A An Installation transaction shall be performed according to figure 6.24.

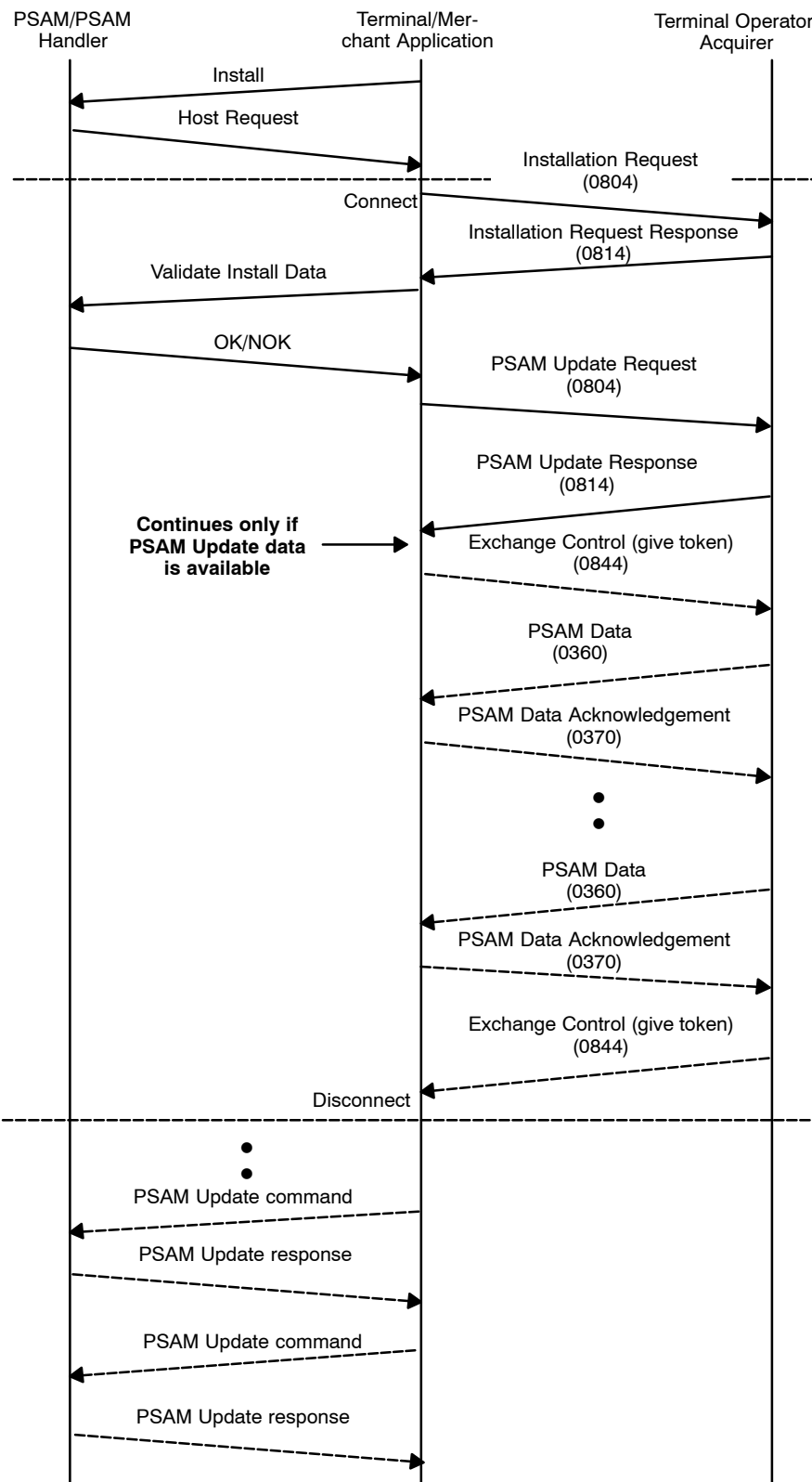


Figure 6.24 – Installation Transaction

- 6.16.2.2 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 shall initiate an Installation transaction whenever a PSAM is physically inserted in a new terminal. See section 6.1.4 for further details.
- 6.16.2.3 A When the merchant initiates an Installation transaction, the MAD-Handler shall provide the following data elements in the *Install* 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
- 6.16.2.4 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.
- 6.16.2.5 A A successful Installation transaction shall be followed by a PSAM Update transaction as defined in section 6.16.7.
- The formats for the Installation messages are defined in Attachment F.

### 6.16.3 Advice Transfer, Advice Enclosing and Advice Forwarding

#### Introduction

Three mechanisms are defined for transfer of advices from the terminal Data Store to the host systems:

- Advice Transfer
- Advice Enclosing,
- Advice Forwarding

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.

Advice Enclosing and Advice Forwarding is utilized to avoid an accumulation of advices in the Data Store.

Advice Enclosing is the mechanism used for transfer of advices while online requests are processed.

Advice Forwarding is the mechanism when the transfer of advices is initiated automatically and not tied to any other event or action.

### General Requirements

- 6.16.3.1 A It shall be possible manually to initiate an Advice Transfer when no card related transaction is in process.
- 6.16.3.2 A A CAT terminal shall be able to automatically initiate an Advice Transfer.
- 6.16.3.3 A If the terminal is capable of performing online requests, either Advice Enclosing or Advice Forwarding shall be supported.
- It is the task of the PSAM to create the complete Advice and to store it in the Data Store. If a Merchant Application Log is supported by the terminal, the PSAM sends a copy to the Merchant Application for logging purposes.
- 6.16.3.4 A The terminal shall send the Advices in the sequence listed below (see figure 6.25):
1. Priority1 file (Reversal Advices (0426))
  2. Priority2 file (Financial Advices (0226))
  3. Priority3 file (Authorization/Reversal Advices (0126, 0426))
  4. Priority4 file (Administrative Advices (0624), e.g. Service Records and Addendum records)
- 6.16.3.5 A The priority for sending the Advices are as indicated above, i.e. the terminal shall send all Reversals before proceeding to Financial Advices and so on. Administrative Advices have the lowest priority and shall only be sent when all the other advice types have been sent.



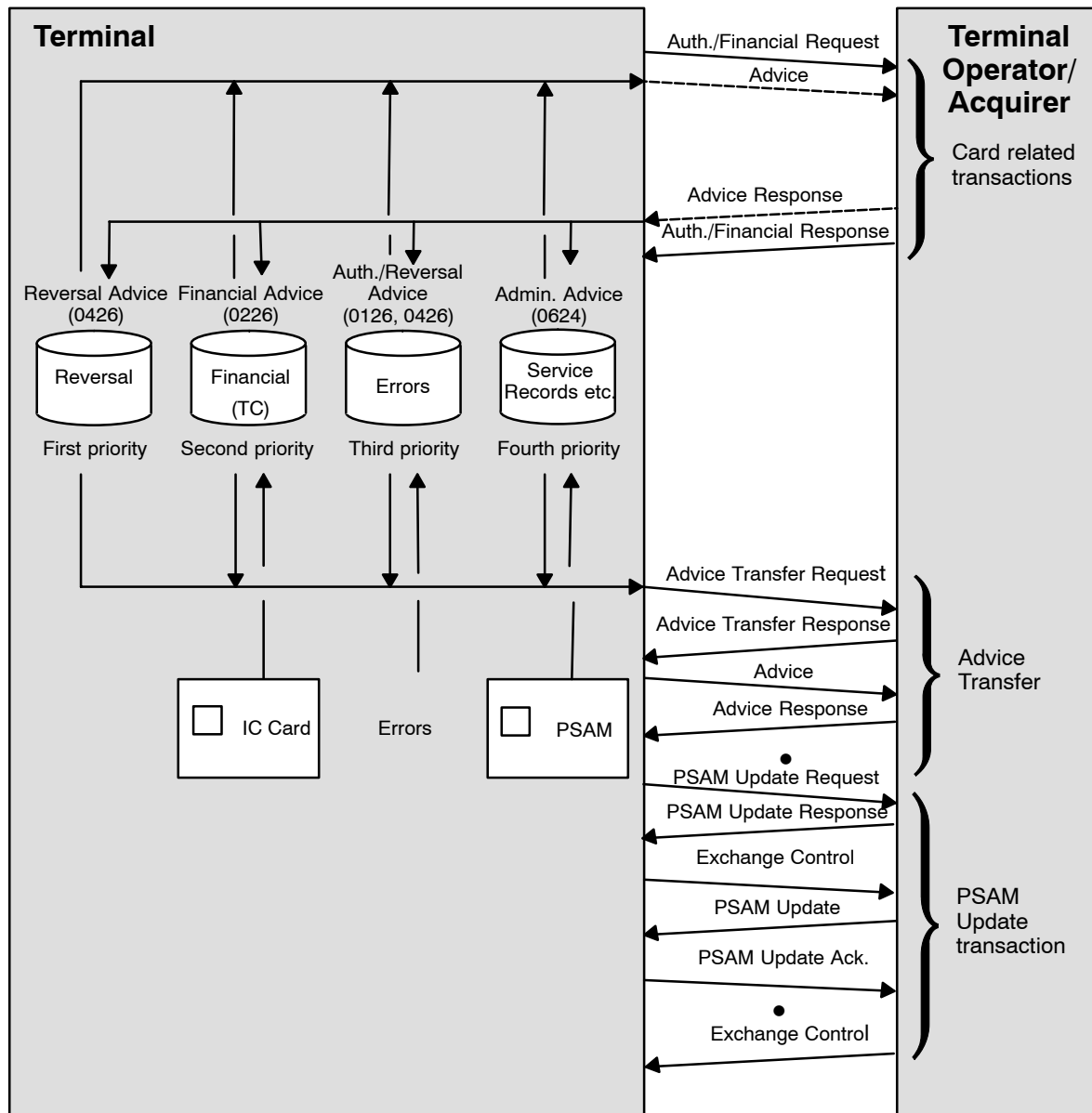


Figure 6.25 – Advice Handling

**NOTE:** Authorization Advices is created only when an error has occurred after an *Initiate Payment* command has been issued and before an online session has been established. Authorization Advices are used to inform the Terminal Operator/acquirer of these incidents.

## 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 6.26.

The PSAM will generate a random number that will be conveyed in field 61 of the Advice. Advices in Data Store is 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.

- 6.16.3.6     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.
- 6.16.3.7     A     The MAD-Handler shall re-compute a new check value using the random number from the Advice Response as input.
- 6.16.3.8     A     The algorithm used to compute the check value shall be SHA-1, according to ref. 33, “Secure Hash Standard”, where the 8 most significant bytes are used as the check value.
- 6.16.3.9     A     The MAD-Handler shall delete the corresponding Advice stored in the Data Store when both 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).
- 6.16.3.10    B     The MAD-Handler shall calculate the check value on the fly using the random number from an Advice Response and, if the check values match, delete the corresponding Advice in the Data Store.

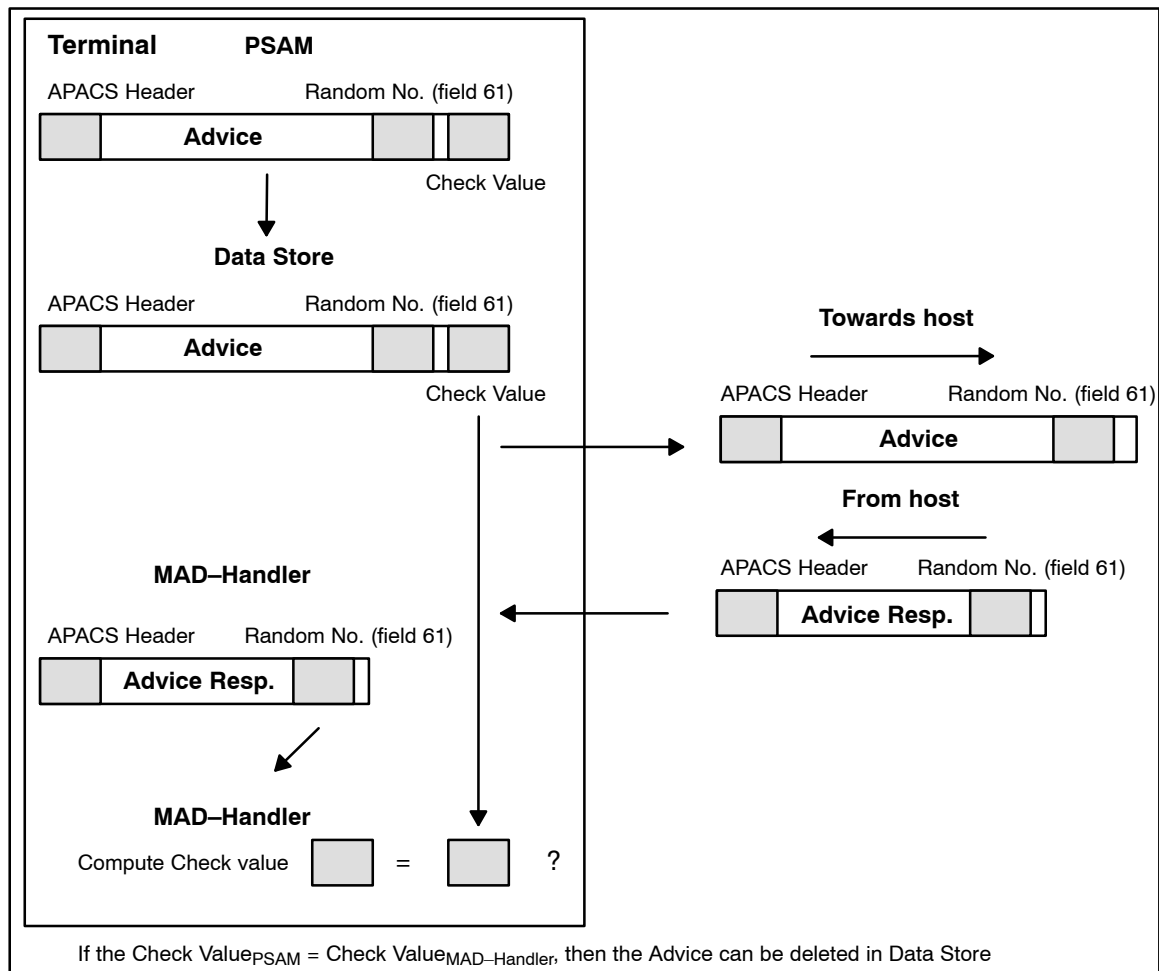


Figure 6.26 – Check Value Handling

### 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 terminal may send before corresponding responses shall be awaited. Advice Window Size is relevant for the transfer of advices only.

The Advice Window Size is controlled by the Terminal Operator’s host as described in Attachment F, while the data element Terminal Advice Window Size is maintained by the terminal. The value of the Advice Window Size depends of the load at the host and may be in the range from 000 to 999.

The format of the Advice Window Size is defined in Attachment F, section F.7.9.

If the Terminal try to sent more outstanding advices than the Terminal Operator Host has indicated in the Advice Window Size the Communication Session may be terminated by the host.

- 6.16.3.11 A The MAD-Handler shall be able to control the number of outstanding Advices i.e. Advices sent but no corresponding response received yet.
- 6.16.3.12 A The MAD-Handler shall be able to handle at least one outstanding Advice.
- 6.16.3.13 A When a new Communication Session is initiated, the Terminal Advice Window Size shall be reset to 001.
- 6.16.3.14 A If the size given in the Advice Window Size in the APACS header is less than the size in the Terminal Advice Windows Size, the MAD-Handler shall alter the Terminal Advice Window Size to a size not greater than the one given in the APACS header.
- 6.16.3.15 C If the Advice Window Size given in the APACS header is greater than the size in the Terminal Advice Windows Size, the MAD-Handler may alter the Terminal Advice Window Size to a size not greater than the one given in the APACS header.
- 6.16.3.16 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.
- NOTE:** Until an Advice Window Size in an APACS header is received with a window size greater than 000, no further Advices must be transmitted.
- 6.16.3.17 A If the Terminal Advice Window Size is 000 and the Advice Window Size given in the APACS header is greater than 000, the MAD-Handler shall alter the Terminal Advice Window Size to a size of at least 001 and not greater than the one given in the APACS header.
- 6.16.3.18 A When the outstanding advices reach the number in Terminal Advice Window Size, no further advices must be transmitted before the outstanding advices again are lesser than the number given in the Terminal Advice Window Size.

#### 6.16.4 Advice Transfer

The merchant can each day, when the clerk changes or when he is requested send an Advice Transfer request to the Terminal Operator system.

The purpose of the Advice Transfer is to allow the merchant to deliver the Advices stored in the Data Store to the Terminal Operator.

- 6.16.4.1 C It may be possible automatically to initiate an Advice Transfer when no card related transaction is in process.
- 6.16.4.2 C It may be possible manually to initiate an Advice Transfer in parallel with card related transactions in process.

- 6.16.4.3 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 F.8.11.

- 6.16.4.4 A The terminal shall not send any advices with the Advice Transfer Request.

- 6.16.4.5 A When the Advice Transfer Request Response have 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 to receive Advices due to heavy load, the host may respond with the Action Code “8421” (Failed, retry, Initiate new connection – deferred, no further details).

- 6.16.4.6 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).

- 6.16.4.7 A The terminal shall carry on sending Advices (if present in the Data Store) as indicated in the Terminal Advice Window Size until all Advices in the Data Store has been sent.

For exception handling during Advice Transfer, see section 6.18.16, “Action Codes” and attachment L, “Defective Advices in Data Store”.

### **PSAM Update**

- 6.16.4.8 B A successful Advice Transfer shall be followed by a PSAM Update transaction as defined in section 6.16.7.

### **Counters and Batch Numbers**

- 6.16.4.9 C When performing the Advice Transfer, counters maintained by the terminal/Merchant Application may optionally be reset.

An example of counter information to be updated during an Advice Transfer can be found in section 6.16.10, “Counters and Batch Numbers”.

The command sequence for an Advice Transfer is described in the figure 6.27.

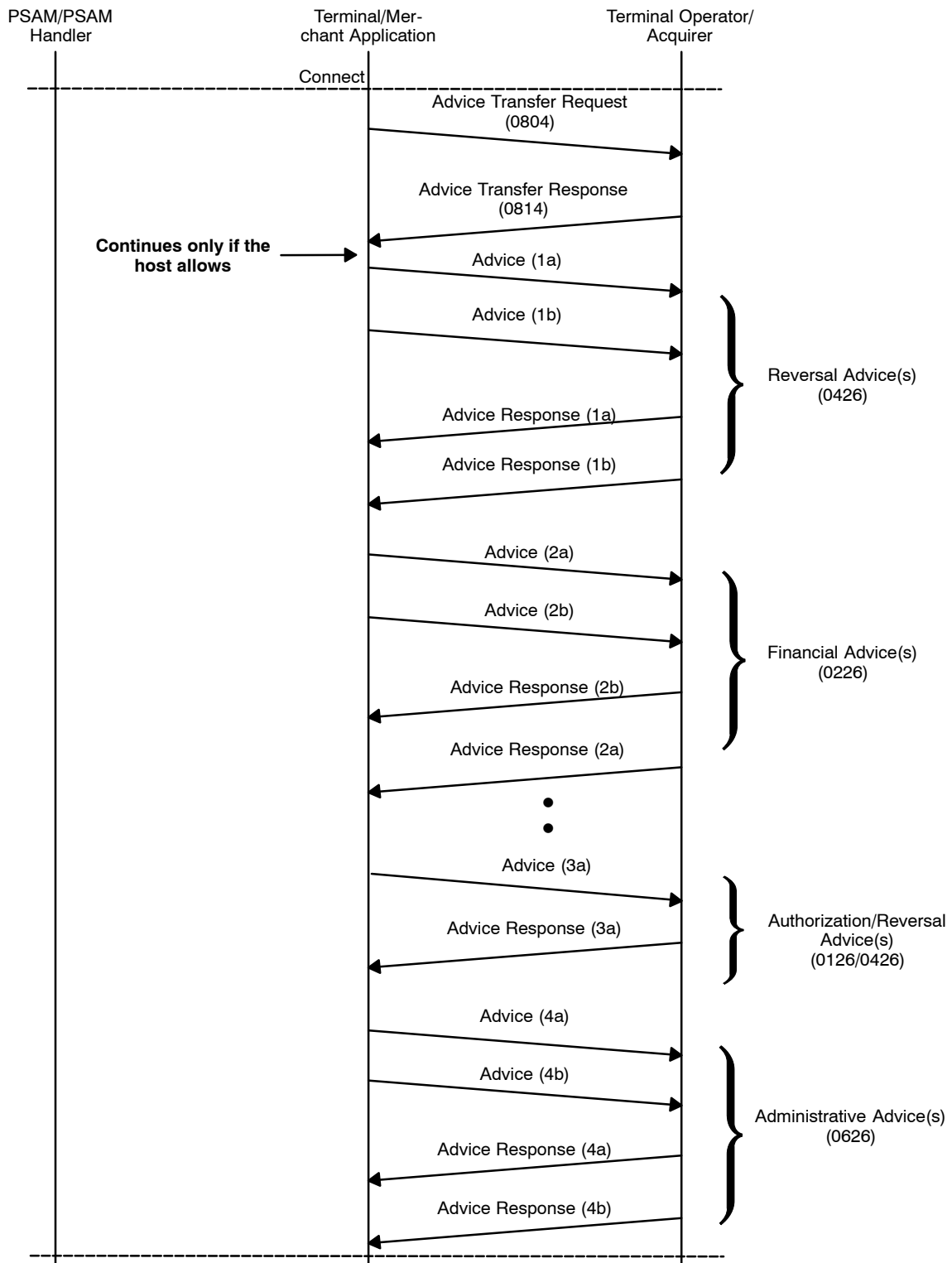


Figure 6.27 – Advice Transfer

The Data Store must not contain any Advices after a successfully completed Advice Transfer, except for the Service Record created after the mandatory PSAM Update.

### 6.16.5 Advice Enclosing

If a switched/dial-up network is used, Advice Enclosing can reduce the communication costs, by utilizing the capability of the network while processing online requests.

- 6.16.5.1 A Immediately after the Financial/Authorization Request has been sent, the MAD-Handler shall send the number of Advices (if present in Data Store) as controlled by the Terminal Advice Window Size.

**NOTE:** Since the default value for Terminal Advice Window Size is 001, no more than one Advice shall be send immediately after the Financial/Authorization Request.

- 6.16.5.2 A The MAD-Handler shall carry on sending Advices (if present in the Data Store) as indicated in the Terminal Advice Window Size, after Advice Responses have been received and processed.

The terminal will receive an Advice Response or an Authorization/Financial Response in random order.

- 6.16.5.3 A After the response to the Financial/Authorization Request is received, the Communication Session shall be maintained until the outstanding Advice Responses are received or time-out detected.

**NOTE:** The Advice Responses may be received in random order, see example 2 in figure 6.28.

- 6.16.5.4 C The MAD-Handler may continue sending Advices (as long as allowed by the Advice Window Size), if the transfer is performed as a ‘background job’ not delaying the actual online transaction.

- 6.16.5.5 B If the transfer of Advices influence on the transaction timing for the actual online transaction, the MAD-Handler shall not send any Advices after the Financial/Authorization Request Response has been received.

Attachment F, table F.9 “Host Generated Data Objects in the APACS Header” gives an overview in which response APACS headers the Advice Window Size may be available.

Figure 6.28 gives two examples of Advice Window Size handling.

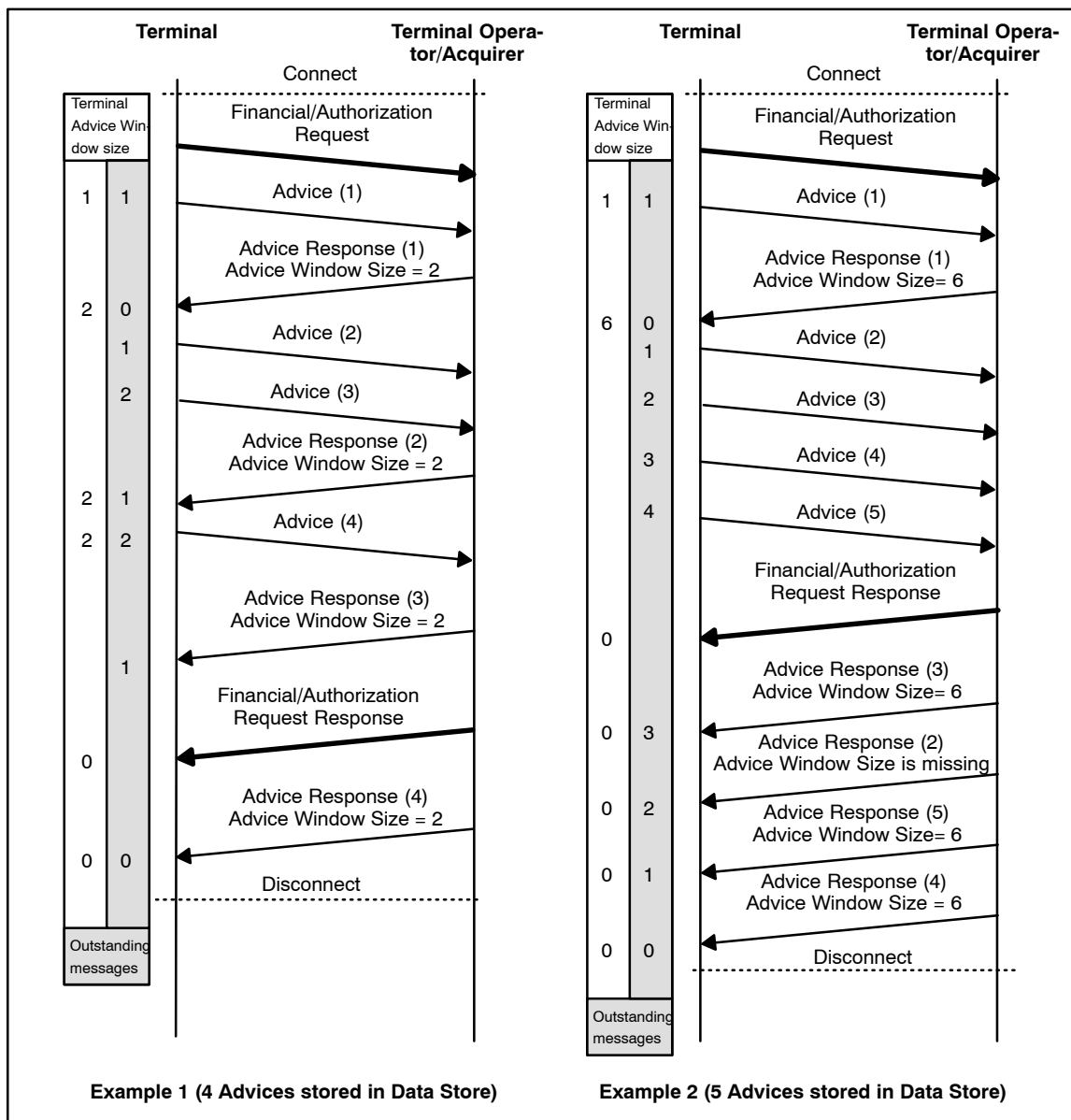


Figure 6.28 – Advice Window Size (Examples)

### 6.16.6 Advice Forwarding

The function Advice Forwarding may be seen as an additional tool for transfer of Advices as a ‘background job’, when it is most convenient for the terminal.

The Advice Forwarding function is an “automatically” initiated Advice Transfer procedure without the initial Advice Transfer Request message.

If the terminal supports Advice Forwarding, the following requirements apply:

- 6.16.6.1 A In case of Advice Forwarding, the Advice Transfer Request (Message Type Identifier = 0804) shall be omitted.
- 6.16.6.2 A Advice Forwarding shall be performed as a ‘background job’ not delaying, disturbing or preventing any transactions.



- 6.16.6.3 A If the terminal receives any message including the data element Advice Window Size with the value 001 or greater, the terminal shall set the Terminal Advice Window Size to 001.

**NOTE:** The Terminal Advice Window Size shall not exceed 001 during Advice Forwarding.

- 6.16.6.4 A If an Advice Forwarding procedure fails, the terminal shall wait at least 15 minutes before initiating a new Advice Forwarding procedure.

### 6.16.7 PSAM Update Transaction

PSAM updates are required whenever data, keys etc. are out-dated 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.

- 6.16.7.1 B The PSAM Update Transaction shall be performed at least once per day. It is recommended to let it follow the Advice Transfer process.
- 6.16.7.2 B A daily PSAM Update transaction shall be initiated automatically.
- 6.16.7.3 C A PSAM Update transaction may optionally be initiated manually e.g. by a Business Call.
- 6.16.7.4 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.
- 6.16.7.5 A The PSAM Update command(s) shall be sent to the PSAM immediately after the disconnection, see figure 6.29.
- 6.16.7.6 C The terminal may sent the PSAM Updates to the PSAM on the fly if possible.
- If the Terminal Operator host is not capable to deliver PSAM Updates due to heavy load, the host may respond with the Action Code “8421” (Rejected, retry, Initiate new connection – deferred, no further details).
- 6.16.7.7 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).

- 6.16.7.8 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.
- 6.16.7.9 A Each command APDU must be forwarded to the PSAM Handler in an “ICC Command” Terminal Message (Message Type ‘42’) as defined in ref.: 40: “TAPA, Application Architecture Specification”.
- 6.16.7.10 A When formatting the terminal message, the terminal Debit/Credit application shall determine the PSAM sub-address from the PSAM Identification.
- 6.16.7.11 A When the MAD-Handler assigns a value for the ID<sub>THREAD</sub> it shall replace the ID<sub>THREAD</sub> value in the command APDU accordingly.
- 6.16.7.12 A In the response to any of the PSAM Update commands, the PSAM may use the ASW1-ASW2 to request that the terminal perform some actions. After processing *all* available PSAM Updates, the terminal must take action prior to initiating any new D/C transactions. Figure 6.31 defines the priority if 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 6.1.

- 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 Attachment F.

### 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.

- 6.16.7.13 A After sending all PSAM Updates, the terminal shall send a *Create Service Record* command to the PSAM.

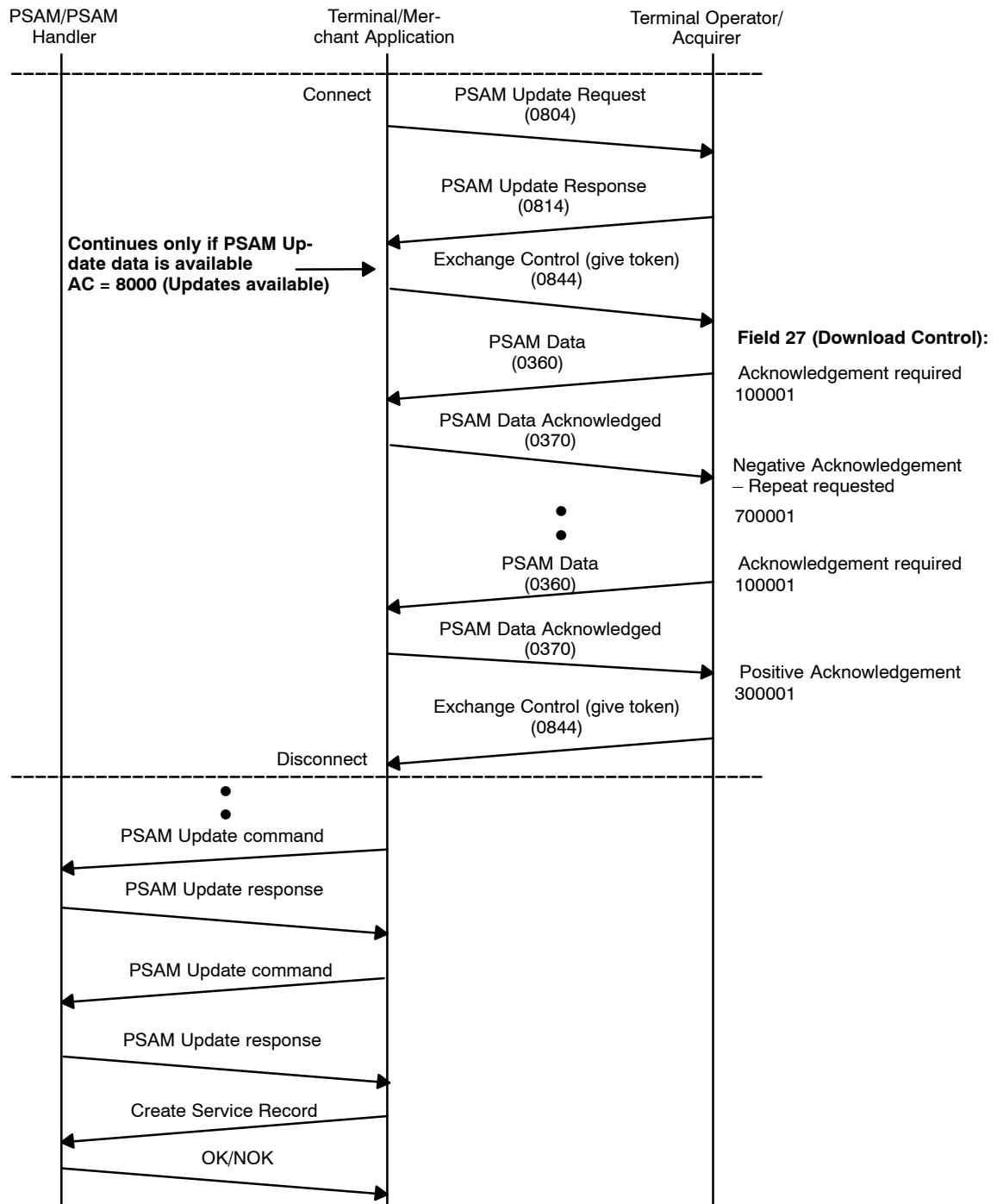


Figure 6.29 – PSAM Update Transaction

### 6.16.8 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.

- 6.16.8.1 A The PSAM Update command(s) (conveyed in PSAM Deactivation Response) shall be sent to the PSAM immediately after the disconnection.

- 6.16.8.2 C The terminal may sent the PSAM Updates to the PSAM on the fly if possible.

The PSAM is not involved in the validation of the PSAM Deactivation Request Response.

The formats for the PSAM Deactivation messages are defined in Attachment F.

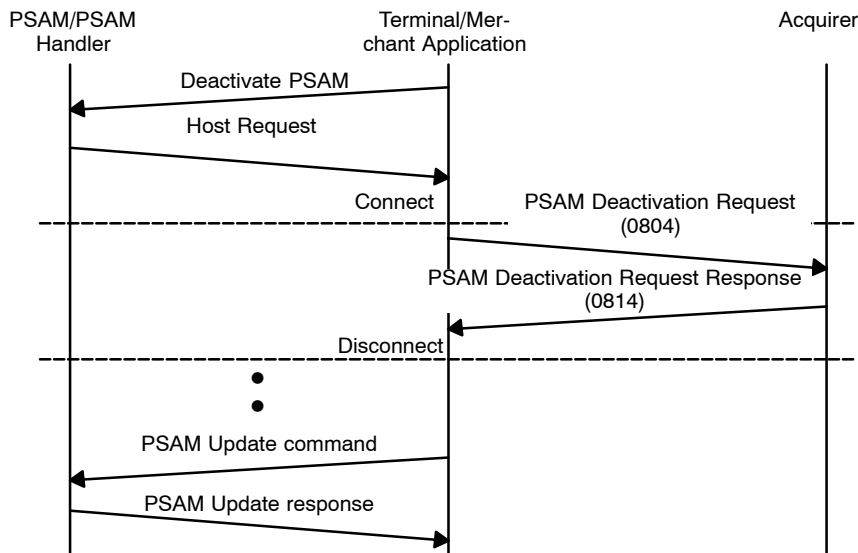


Figure 6.30 – PSAM Deactivation Transaction

### 6.16.9 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 timestamp 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 Attachment F.

### 6.16.10 Counters and Batch Numbers

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 6.17. Examples of values for Reconciliation counter id and Reconciliation counter name can be found in Attachment F, section F.9.10.

The Batch Number (Retrieval Reference Number, field 37) is maintained by the merchant.

**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.

6.16.10.1 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 6.17 – 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.

## 6.17 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.

### 6.17.1 Advice Request Flag

The Advice Request Flag may be included in the APACS header and allows the host to request the terminal to initiate an Advice Transfer and a following PSAM Update transaction.

The Advice Request Flag may be present in the headers indicated in Attachment F, table F.7 “Presence of Data Objects in the APACS Header”.

- 6.17.1.1 A When the MAD–Handler receives an Advice Request Flag set in the APACS header, the terminal shall indicate to the merchant that an Advice Transfer and PSAM Update transaction shall be initiated.

**NOTE:** The terminal shall not be “locked” until an Advice Transfer has been initiated. It is only the message to the Merchant that shall be displayed before any card related transaction may be initiated.

Advice Request Flag is defined in Section F.7.10.

### 6.17.2 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.

### 6.17.3 Repeat Messages

In case a request or advice message is resend, 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 Action Instruction Acknowledge, Message Type Identifier = 0370.

- 6.17.3.1 A If the terminal does not receive a response to an original request (Message Type Identifier = 0106 & 0206) or Network Management Request (Message Type Identifier = 0804), the terminal shall “mark” the message to indicate repeat before sending the request again.
- NOTE:** In all subsequent sendings the request shall indicate repeat.
- 6.17.3.2 A The terminal shall “mark” an advice as a repeat, if not already “marked” as a repeat, after the terminal has read the advice from the Data Store in order to send it online.
- 6.17.3.3 B The marking of advice messages as repeats shall be performed by sending an *Update File Record* command to adjust the advice stored in the Data Store.

#### 6.17.4 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 following deny all attempt to connect to the access points for a given time interval before the connections attempt will be accepted again.

Section E.3 defines the communications networks and protocols supported.

- 6.17.4.1 A If the processing in the terminal indicates that exchange of messages is going to be performed and no Communication Session is open already, the terminal shall initiate a new Communication Session.



- 6.17.4.2 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.
- 6.17.4.3 A If one Communication Session is initiated the terminal shall not initiate a new session until the previous has been closed.
- 6.17.4.4 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.
- 6.17.4.5 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.
- 6.17.4.6 A TCP connection shall be established when a Communication Session is initiated.
- 6.17.4.7 A The TCP connection shall be closed when the Communication Session is closed.
- 6.17.4.8 A During a Communication Session the messages exchanged shall be transferred in an even flow without unnecessary delays.
- 6.17.4.9 A The terminal shall be able to detect if an open Communication Session is interrupted unexpected.
- 6.17.4.10 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.
- 6.17.4.11 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.
- 6.17.4.12 A If there still are outstanding responses and no further 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.
- 6.17.4.13 A When a time-out is detected the terminal shall interrupt the actual Communication Session.
- NOTE:** If other responses are outstanding, the terminal shall await all responses or time-outs before closing the session.

### 6.17.5 Terminal Operator Communication Access Points

To be able to offer the highest level of availability, the Terminal Operator may support more than one access points. Each access point has its own IP address and in case a switched network is used, each access point has its own dial-up numbers too.

A transaction may be initiated by either a Business Call or administrative routines.

- 6.17.5.1 A The terminal shall be able to initiate Communication Sessions to at least two access points.
- 6.17.5.2 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.
- 6.17.5.3 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.

## 6.18 Exception Handling

### 6.18.1 Introduction

There are a variety of exception conditions that can occur during the dialogue between the terminal and the 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. 40: “TAPA; Application Architecture Specification”, section 4.3.

### 6.18.2 General Rules

#### Actions to be taken upon ASW1–ASW2

Figure 6.31 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 8.8.1.

**NOTE:** Figure 6.31 does only cover ASW1–ASW2 values which require special action.

- 6.18.2.1     A     If the PSAM respond with an ASW1–ASW2 indicating an unsuccessful operation to a command or the MAD–Handler encounter 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<sub>THREAD</sub> and return to idle. At the same time the *Transaction Completed* command shall be send to the Merchant Application indicating that the transaction failed.

**NOTE:** The PSAM can be considered “cleaned–up” (and the ID<sub>THREAD</sub> released) when a successful response to the *Complete Payment* command is received.

**NOTE:** If the PSAM respond 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.

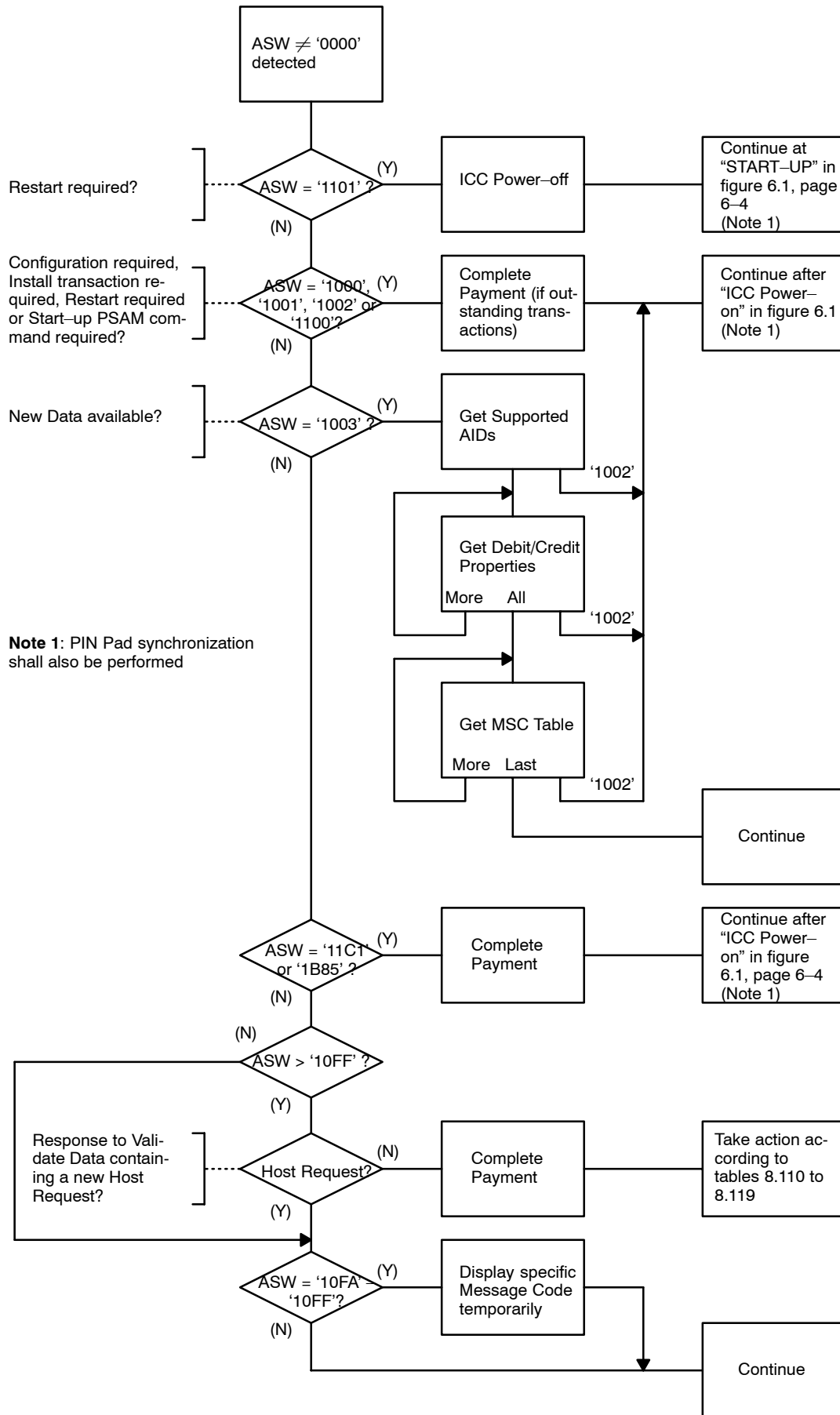


Figure 6.31 – Handling of ASWs which Requires Special Action

Three main categories of errors exists:

### **Errors occurring before the selection of the terminal application**

- 6.18.2.2 A The MAD–Handler shall indicate the type of error in one of the error counters specified in Attachment F, section F.6 “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 when an online connection has been established.**

Either the host, card or PSAM may decide to decline the transaction. No Authorization Advice shall be created, but in the case where the PSAM/card declines an approved transaction from the host, the PSAM will create a Reversal.

If an error occurs during an offline transaction, the PSAM will create an Authorization Advice.

## **6.18.3 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

## **6.18.4 Terminal Related Errors**

### **Installation/Start–up**

- 6.18.4.1 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, all 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

- |   |          |   |  |
|---|----------|---|--|
| ■ | 6.18.4.2 | A | In case of erroneous reading of an EMV card, the exception handling shall follow rules defined in ref. 36: “EMV, version 4.1”, section 2.5.2 of the terminal part.   |
| ■ | 6.18.4.3 | A | Exception handling related to online Authorizations and Advices in case of an EMV card shall follow the requirements given in ref. 36: “EMV, version 4.1”, section 2.2 of the terminal part.                   |
|   | 6.18.4.4 | 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

- |  |          |   |   |
|--|----------|---|---|
|  | 6.18.4.5 | A | If a communication error occur 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

- |  |          |   |   |
|--|----------|---|---|
|  | 6.18.4.6 | 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"> <li>• Attempt to complete all in-progress transactions (by sending a <i>Complete Payment</i> command for each current IDTHREAD).</li> <li>• Attempt to shutdown the PSAM application “gracefully” by sending the <i>PSAM Shutdown</i> command.</li> </ul> |
|--|----------|---|---|

## 6.18.5 PSAM Related Errors

### Installation/Start-up

- 6.18.5.1 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 *Start-up PSAM* command.

### PSAM Updates

- 6.18.5.2 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')
- 6.18.5.3 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.

## 6.18.6 Host Declined Transactions (Requests)

### 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 6.32. The ASW1-ASW2 returned in the response to *Validate Data* command is '10FF' ("Incorrect PIN") when a new try is performed.

- 6.18.6.1 A Whenever the response to the *Validate Data* command contains a length field  $LEN_{STAN+HREQ}$  different from '0000', the terminal shall send the entire host request.

**NOTE:** The response to the *Validate Data* command contains a new host request only, if the use of 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* command, see page 8–43.

**NOTE:** 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.

**NOTE:** 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.

- 6.18.6.2     A     If a new host request is generated, the terminal shall initiate a renewed *Validate Data* command when the response to the host request is received according to the example given in figure 6.32.

**NOTE:** The handling of a new host request has priority to the Application Status Words (ASW1–ASW2).

**NOTE:** In case of PIN retry, several different host requests may be expected each containing an unique STAN.

**NOTE:** 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.

- 6.18.6.3     A     Receipts shall be printed according to Attachment G.



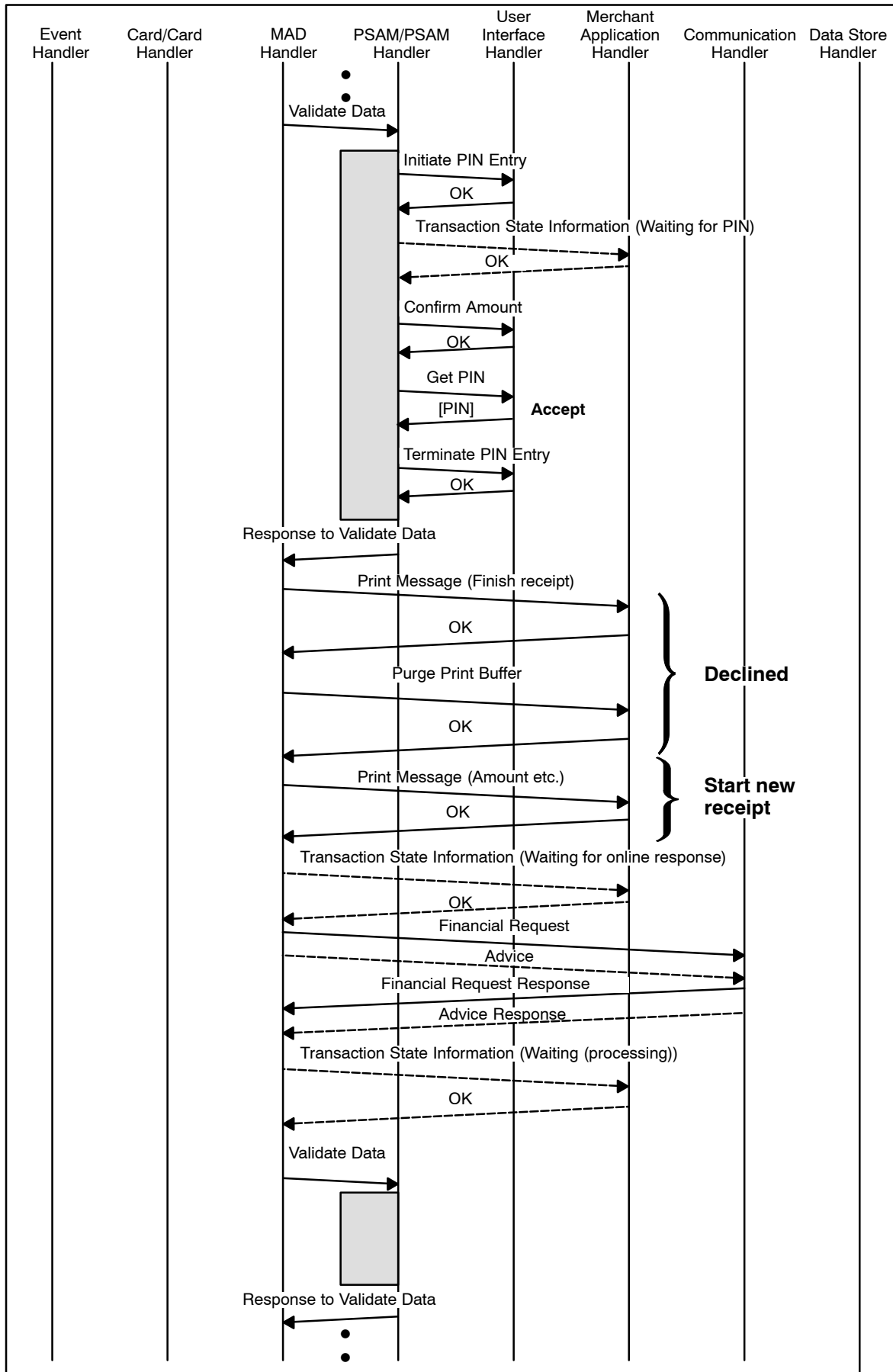


Figure 6.32 – PIN Retry Flow

### 6.18.7 Host Declined Transactions (Advices)

An Advice may not be accepted by the host or the terminal may not be able to accept the Random Number received.

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

#### Action Code

The Action Code returned by the host indicates the action(s) to be taken by the terminal and/or the merchant.

If the host response is processed by the PSAM, the ASW1–ASW2 received subsequently from the PSAM takes priority to the Action Code.

If the processing is handled solely by the terminal, the mapping between Action Codes and the Message Codes to display and/or print is defined in section 6.18.15, “Error Messages”.

#### Advices Enclosing and Advice Forwarding

- 6.18.7.1      A      If the Advice is still not accepted after two retries, the terminal shall finish the current transaction, but shall not be able to perform any Debit/Credit transactions before an Advice Transfer has been initiated.

**NOTE:** Communication errors shall not cause the terminal to be unable to perform further transactions.

#### Advice Transfer

- 6.18.7.2      A      If an Advice is not accepted by the host, the terminal shall try to re-send the Advice twice, before handling the next Advice in the files.
- 6.18.7.3      A      If the Data Store contains not accepted Advices after the Advice Transfer, a technician shall be alerted. The terminal shall not initiate further Debit/Credit transactions.

### 6.18.8 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.

### 6.18.9 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.

### 6.18.10 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.

### 6.18.11 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)

The cancellation is initiated during the *Get Amount* command and this command was 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.

- |           |   |   |
|-----------|---|---|
| 6.18.11.1 | A | The Cancel button shall be active until the cardholder has confirmed the amount (and for PIN related transactions, both amount and PIN).  |
| 6.18.11.2 | 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. |
| 6.18.11.3 | A | If the cancellation is initiated during the <i>Get Amount</i> 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 11.2 on page 11–7 for further details concerning the behavior of the different variants of the *Get Amount* command.

- 6.18.11.4 A If any subsequent *Get Amount* command is issued after the cancellation is initiated as defined in requirement 6.18.11.3, the response shall contain the Response Code ‘FFF2’ as well.
- NOTE:** Subsequent *Get Amount* commands may occur in the situations described in section 11.4.2. Although this section refer to the *Get Amount 2* command, the principle is valid for the *Get Amount* command too.
- 6.18.11.5 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.
- 6.18.11.6 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”.

## 6.18.12 Communication Statistics and Error Counters

See description in Attachment F, section F.6 and F.9.11 respectively.

## 6.18.13 Authorization Advice

An Reversal Advice or Authorization Advices will be created by the PSAM whenever an error has been encountered by the PSAM. Authorization Advices are created in order to inform the host of the particular error related to a certain card.

## 6.18.14 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 8.8.1, table 8.107 to table 8.119.

## 6.18.15 Message Codes

- 6.18.15.1 A In case of a rejected transaction, the display/print Message Code shall conform to the guidelines given in section 8.8.1 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.

### 6.18.16 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.

**NOTE:** 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 G.1.2.

- 6.18.16.1 C The terminal shall evaluate position 2 of the Action Code in order to determine the subsequent action (see Attachment F, table F.89.)

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 Attachment F.

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 on-line 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 6.18.

Table 6.18 – Action Codes (National Use)

Action Code	Description	Message Code	Text (Merchant Display)
8000	Accepted/Successful	'03'1)	“Godkendt”
8001	Accepted, unspecified mismatch in data	'03'1)	“Godkendt”
8002	Accepted, format error (e.g. MAC error)	'03'1)	“Godkendt”
8003	Accepted, card data mismatch	'03'1)	“Godkendt”

8004	Accepted, merchant data mismatch	'03' <sup>1)</sup>	"Godkendt"
8005	Accepted, PSAM ID mismatch	'03' <sup>1)</sup>	"Godkendt"
8020	Rejected	'07' <sup>1)</sup>	"Afvist"
8421	Rejected, try again later	'07' <sup>1)</sup>	"Prøv igen"
8022	Rejected, format error (e.g. MAC error)	'07' <sup>1)</sup>	"Afvist"
8023	Rejected, card data mismatch	'07' <sup>1)</sup>	"Afvist"
8024	Rejected, merchant data mismatch	'07' <sup>1)</sup>	"Afvist"
8025	Rejected, PSAM ID mismatch	'07' <sup>1)</sup>	"Afvist"
<b>Legend:</b>			
1) May not be displayed (transfer may run in the "background").			

## 6.18.17 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 the present transaction.

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.

- 6.18.17.1 C The cancellation shall be indicated in the respective responses as defined when activating the Cancel button on the User Interface (see section 6.18.11).

## 6.18.18 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.

- 6.18.18.1 A If a time–out value expires while awaiting either amount entry, PIN entry or amount confirmation, a cancellation shall be initiated.

**NOTE:** The cancellation may be seen as a parallel to activating the Cancel button on the User Interface.

- 6.18.18.2 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.

- 6.18.18.3 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).

- 6.18.18.4 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”.

- 6.18.18.5 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”.

This page is intentionally left blank



# 7. Best Practice

## 7.1 Introduction

The purpose of this chapter is to list a number of useful hints and guidelines for both Flexterminal developers and developers of cash register systems interfacing Flexterminals.

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.

## 7.2 Documentation

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

This manual shall contain sufficient information making the staff able to operate system concerning card payments and settlements.

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

## 7.3 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 Flex-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.

## 7.4 Choice of Business Call

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

Six 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 Business Call

- “Purchase”
- “Refund” (in case of credit transactions)

Concerning surcharges, please refer to section 7.24 (Addition of Surcharges and Fees).

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

- “Original Authorization”,
- “Supplementary Authorization”,
- “Capture” and
- “Reversal (Authorization)”

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

(Support of Supplementary Authorization depends on the individual card schemes. Currently not supported by any card schemes).

### References

Business Calls, definition: Section 6.2 (Business Calls) on page 6–14.

Terms – Business Calls and Administrative Functions: Attachment K.33

## 7.5 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 or quasi-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 6.2.6 on page 6–19.

## 7.6 Support of Card Technologies

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

- ICC,
- Magnetic Stripe (Track 2) and
- Key–Entered

Presently, Key–Entry of card data is not supported.

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 9.2.15 on page 9–5.

## 7.7 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 will reject the attempt and request the cardholder to use the ICC reader instead.

### References

Fallback, description: Section 5.14 (Fallback from Chip (ICC) to Magnetic Stripe (MSC) on page 5–33.

Card inserted correctly: Section 5.14.2 on page 5–33.

## 7.8 Service Packs

In order to add new variants of existing commands and responses, the term Service Pack has been introduced.

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

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

### References

Service Packs: Section 6.1.3 (Restart) on page 6–6

Service Packs: Section 11 (Service Packs)

## 7.9 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.

### References

Application Selection: Section 5.13 (Application Selection) on page 5–22.

## 7.10 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
- (or 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 (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.

Dependent of which goods and services an unattended terminal delivers, PIN and/or No CVM may be supported.

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: Attachment O (Merchant Initiative Bypass).

Merchant Initiative, definition: Section 9.2.54 on page 9–13.

## 7.11 Temporary Offline Procedure

Card processing performed by the PSAM may imply that an on-line 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 a 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. making a phone call to acquirer's helpdesk, this may more or less compensate for the reduces guarantee.

How to obtain an Approval Code in case of temporary offline is described in section 7.12.

### References

Merchant Initiative, definition: Section 9.2.54 on page 9-13.

## 7.12 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 (paper based) 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 (paper based) Stop List.
- Authorization Call performed, but the authorization request has been declined,
- 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 key-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. 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 origin 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 6.10.4 (EMV Payment) on page 6–44 and section 6.12.4 (MSC Payment) on page 6–70.

## 7.13 Stop List

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

Normally the Stop List will be stored on the merchant operated part of the terminal solution, normally in the cash register system.

Updates to the Stop List, as well as a complete Stop List, shall be obtained directly from PBS by calling the dedicated platform for Stop List information. Normally it will be the cash register system that maintains the Stop List.

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

- If the actual card is an EMV card (also during online transactions), or
- 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) or just returned to the cardholder.

### References

*Check Stop List* command: Section 8.6.18 on page 8–71.

## 7.14 Optimizing the Transaction Time

### 7.14.1 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 contents is known and ICC data may be read by the terminal/PSAM while the merchant is calculating 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 such “Accelerated PIN Entry” (APE/DAPE) have been implemented in newer PSAM versions 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 6.14, 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 6.11.3 (Release of the ICC) shall be followed.

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

## **7.14.2 Data Transmission**

### **Clock Frequency**

For both the ICC and PSAM interfaces, it is recommended to use the maximum frequency of 5 MHz. as defined in ref. 8: “ISO/IEC 7816–3” and ref. 36: “EMV, version 4.1”.

In this way, ICCs using the external clock for clocking the CPU will operate faster compared to the widely used frequency of 3.57 MHz.

Furthermore, data transmission to and from ICCs takes place at a bitrate directly proportional to the external clock frequency.

**NOTE:** Although the PSAM generates its own clock frequency internally, the overall transaction time will still benefit from a faster transmission rate when clocked at 5 MHz.

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

Terminal I/O buffer(s) 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)**

Terminal I/O buffer(s) should have sufficient length to avoid chaining at the T=1 level. This is especially the case for the PSAM interface where several messages during a transaction have the maximum size (length of the INF field is 254 bytes).

Terminal I/O buffer sizes different from the default value of 32 bytes shall be indicated to the ICC/PSAM by use of an S(IFS request) message issued after ATR and possibly PPS.

#### **Transmission Factors F and D (ICC interface)**

The time spent on data transmission on the ICC interface may be reduced for cards supporting bit rate adjustment factors (called “D”) other than 1. Ref. 36: “EMV 4.1” requires terminals to support the values 1, 2 and 4 and cards to support the value 1 and optionally 2 and/or 4.

The method for negotiating values for F and D is Cold/Warm Reset.

#### **Transmission Factors F and D (PSAM interface)**

The time spent on data transmission on the PSAM interface may be significantly reduced when supporting bit rate adjustment factors (called “D”) other than 1.

All PSAMs used for production support the values 1, 2, 4 and 12.

Presently, only FI=1 is supported by the PSAM indicating  $f_i=372$  and  $f_{max}=5$  MHz

The method for negotiating values for F and D is PPS (“Protocol and Parameters Selection”) as defined in ref. 8: “ISO/IEC 7816-3”.

#### **References**

Optimizing the Transaction Time: Section 6.11 (Optimizing the Transaction Time) on page 6-54.

## **7.15 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 6.4.2 (Signature) on page 6–26.

## 7.16 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 Accept–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. The cardholder receipt can therefore 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 Accept key when the amount appears in the display.

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

The terminal may print receipts in case of errors, rejections, cancellation, etc., even though a receipt is not required.

### References

Receipts: Attachment G (Receipts)

## 7.17 Get Amount 2

Depending on the actual ICC card, the PSAM may request the amount to be determined at a very early stage of the transaction flow, and even before the card number (PAN) is known.

If the terminal supports Service Pack No. 1 (i.e. the *Get Amount 2* command is issued by the PSAM), the PAN-prefix will not be available in the command, in this situation. The field PAN-prefix will in this situation contain 4 bytes, each with the value '00'.

If the PAN-prefix is not available in the *Get Amount 2* command (during an EMV transaction), and the terminal must know the actual type of card before the exact transaction amount can be determined, the terminal may generate a response saying that 'the amount is not yet known'. Based on this response the transaction sequence will continue, and a second *Get Amount 2* command will be issued later on during the transaction, after the PAN-prefix is known.

### References

*Get Amount 2* command: Section 11.4.2 (Get Amount 2).

## 7.18 Get Amount 3

If the PAN is unknown when the ICC card request the amount and the terminal supports Service Pack No. 2 (i.e. the *Get Amount 3* command is issued by the PSAM), the PAN will not be available in the command, in this situation. The  $LEN_{PAN}$  will in this situation be equal to '00' and the data element "Amount Request" will indicate "Initial Amount" It is then up to the terminal/Cashregister System to return either an estimated amount or an accurate amount.

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

### References

*Get Amount 3* command: Section 11.5.1 (Get Amount 3) on page 11-5.

## 7.19 Transaction Result

During the processing of a transaction, the terminal sends 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 8.106.

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 6.18.2 (General Rules) on page 6–143 and section 8.8 (ASW1–ASW2 Coding) on page 8–92.

## 7.20 Transaction Checks

The PSAM offers two different features for avoiding 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 PANs are identical
- The amounts and currencies are identical
- The same type of Business Call is used (Purchase, 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.

### **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**

Attachment Q (Status of Previous Transactions).

## **7.21 Log and Totals**

A transaction log shall be maintained within the terminal or an interfaced cash register. The transaction log may either be stored in the terminal or in a cash register system interfaced to the terminal.

The transaction log is not only relevant for audit purposes and technical trouble-shooting, but also for settlement purposes and 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 host systems, 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 indication of the actual settlement period.

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

### References

Log: section 5.4.3 (Log) and Attachment N (Guidelines for Constructing Total Reports).

## 7.22 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 6.1.3 (Restart) on page 6–6.

## 7.23 Cashback Amount

The merchant may (depending on the agreements with the card schemes) 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.

Currently, cashback is not supported by the host. Therefore, the data element Amount Other shall not contain any amount and the Transaction Type = '09' is not valid.

Despite cashback is not supported currently, the terminal may be able to invoke this functionality.

### **References**

Cashback, definition: Section 9.2.7 (Amount, Other) on page 9-3.

## **7.24 Addition of Surcharges and Fees**

The merchant (or the cash register) may add surcharges or other fees to the amount summed up for the goods or services.

Surcharging 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 surcharging and other fees.

### **References**

Surcharges and Fees: Section 6.3 (Gratuity and other surcharges) on page 6-20.

## **7.25 Gratuity**

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

Like for surcharges and fees, the total amount displayed during PIN entry shall include any gratuity. It means that 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 6.3 (Gratuity and other surcharges) on page 6-20.



## 7.26 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, PBS has established two identical platforms. Each platform has its own communication lines to the external communication networks. Both platforms are active 24 hours per day.

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

To be able to utilize the increased availability, obtained 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 platform is inaccessible.

### References

Terminal Operator Communication Access Points: section 6.17.5 and Dual access points: Section F.3 (Communication Protocols).

## 7.27 Automatic Advice Transfer if no Customers being Serviced

For attended terminals an Advice Transfer is normally initiated by the merchant or as a result of an action performed by the merchant, e.g. log-in/Log-out to the cash register.

An Advice Transfer shall be initiated frequently, and at least once a day. An Advice Transfer initiated by the merchant is fol-

lowed 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.

The Advice Transfer is also defined as the function to initiate balancing. Beyond that the Advice Transfer also contributes to minimize the risk for losing any advices while stored in the Data Store.

Further improvements for minimizing the risk for losing advices may be implemented, e.g. if the terminal automatically initiates an Advice Forwarding, a predefined number of minutes after the last transaction has been performed.

In this situation the Advice Forwarding shall not be initiated if the Data Store is empty, likewise the PSAM Update sequence shall be omitted.

The purpose of this automatic initiated Advice Forwarding is exclusively to empty the Data Store, not to initiate any balancing or PSAM update sequences.

### References

Advice Transfer: Section 6.16.4 (Advice Transfer), 6.16.5 (Advice Enclosing) and 6.16.6 (Advice Forwarding).

## 7.28 Host Messages

Each response from the host may contain additional information addressed to the merchant.

The Host has the possibility to add a text message to the Merchant Display (Tag 'CA'), or a request for an Advice Transfer (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 e.g. a request for Advice Transfer is received.

### References

Section F.7 (Primitive Data Objects for the APACS Header) on page F-14.

## 7.29 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 6.1.3 (Restart) on page 6–6.

Transaction State Information, command: Section 8.6.21 on page 8–76.

## 7.30 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

Attachment P (Local PIN).

Commands: Section 8.7 (Local PIN Commands) on page 8–86.

Data Elements: Section 9.3 (Data Elements specific for the Local PIN Application) on page 9–25.

ASW1–ASW2: Section 8.8.2 (ASW1–ASW2 Applicable for Local PIN) on page 8–138.

## 7.31 Certification

The basic certification of EMV functionality (level 1 & 2) shall be performed by an EMV accredited test house e.g. Delta in Denmark.

Before an EMV level 2 certification is initiated, the terminal vendor shall determine the number of business and technical functions supported e.g. PIN code, signature, attended/unattended (stated in an Implementation Conformance Statement (ICS)).

Each terminal or terminal solution shall subsequently be certified according to the requirements defined by the card schemes and the requirements stated in the OTRS.

A terminal may be certified as a stand alone terminal. A terminal can also be a part a terminal solution interfacing a cash register system.

If a terminal solution is based on a previously certified terminal, a supplementary certification of the complete solution is required. The volume of the supplementary certification depends on the level of new and not yet certified hardware and software components.

When an EMV level 2 certified terminal is part of terminal solution, the terminal solution shall support the same number of business and technical functions as defined for the terminal.

## 7.32 Cash/Quasi-Cash Terminals

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

Table 7.1 – Cash/Quasi-Cash Terminals

Terminal Type	Transaction Type	Trade
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/Quasi-Cash Terminals have the following limitations:

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

Table 7.2 – Cash/Quasi-Cash – Applicable Business Calls

Terminal Type	Purchase	Original Authorization	Capture
11 (Cash, Financial Institution)	●	●	●
21 (Quasi-Cash)	●		

## 7.33 POS Terminal/CAT Levels vs. Terminal Type

The following four tables (7.3 – 7.7) can be used to find the outer boundaries for a specific Terminal Type regarding offline/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 PBS before finalizing the terminal functionality design.

**NOTE:** Signature only terminals are *not* allowed according to MasterCard International and Visa International rules.

Table 7.3 – Online/Offline Transactions Vs. Terminal Type

Transaction Terminal Type		MSC		ICC		Key–entered	
		Online	Offline	Online	Offline	Online	Offline
<b>Attended – Financial Institution controlled</b>							
11	Online	●		●			
12	Online capable						
13	Offline						
<b>Unattended – Financial Institution controlled</b>							
14	Online						
15	Online capable						
16	Offline						
<b>Attended – Merchant controlled</b>							
21	Online	●		●			
22	Online capable	●	●	●	●		
23	Offline						
<b>Unattended – Merchant controlled</b>							
24	Online	●		●			
25	Online capable	●	●	●	●		
26	Offline		●		●		
<b>Unattended – Cardholder controlled</b>							
34	Online						
35	Online capable						
36	Offline						
<b>Legend:</b> ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.							

Table 7.4 – CVM Vs. Terminal Type

CVM		PIN		Signature <sup>1)</sup>		No CVM	
Terminal Type		Online <sup>2)</sup>	Offline <sup>2)</sup>	Online	Offline	Online	Offline
<b>Attended – Financial Institution controlled</b>							
11	Online	●		● <sup>3)</sup>			
12	Online capable						
13	Offline						
<b>Unattended – Financial Institution controlled</b>							
14	Online						
15	Online capable						
16	Offline						
<b>Attended – Merchant controlled</b>							
21	Online	●		●			
22	Online capable	●	●	●	●	●	●
23	Offline						
<b>Unattended – Merchant controlled</b>							
24	Online	●					
25	Online capable	●	●			●	●
26	Offline						●
<b>Unattended – Cardholder controlled</b>							
34	Online						
35	Online capable						
36	Offline						
<p><b>Legend:</b> ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.</p> <p>1) = Signature only terminals are not allowed.</p> <p>2) = Indicates whether the transaction has been performed online or offline. Does <i>not</i> implicate whether online PIN verification or offline PIN verification is performed.</p> <p>3) = In case of Cash terminals, the use of signature as CVM can be disabled by PBS.</p>							

Table 7.5 – Transaction Request Vs. Terminal Type

Transaction Request		Purchase	Refund <sup>1)</sup>	Org. Auth.	Supp. Auth.	Capture	Rev. (Auth.)
Terminal Type		'00'	'01'	'02'	'03'	'04'	'05'
<b>Attended – Financial Institution controlled</b>							
11	Online	●		●		●	●
12	Online capable						
13	Offline						
<b>Unattended – Financial Institution controlled</b>							
14	Online						
15	Online capable						
16	Offline						
<b>Attended – Merchant controlled</b>							
21	Online	●					
22	Online capable	●	●	●		●	●
23	Offline						
<b>Unattended – Merchant controlled</b>							
24	Online	●		●		●	●
25	Online capable	●		●		●	●
26	Offline	●					
<b>Unattended – Cardholder controlled</b>							
34	Online						
35	Online capable						
36	Offline						
<p><b>Legend:</b> ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.</p> <p><sup>1)</sup> = For Cash terminals, Refund transactions are not allowed.</p>							

Table 7.6 – Transaction Type Vs. Terminal Type

Transaction Type		Goods & Services	Cash <sup>1)</sup>	Goods & Services with Cash-disbursement	Quasi-Cash and scrip	Returns/Refunds
Terminal Type		'00'	'01'	'09'	'11'	'20'
<b>Attended – Financial Institution controlled</b>						
11	Online		●			
12	Online capable					
13	Offline					
<b>Unattended – Financial Institution controlled</b>						
14	Online					
15	Online capable					
16	Offline					
<b>Attended – Merchant controlled</b>						
21	Online				●	
22	Online capable	●				
23	Offline					
<b>Unattended – Merchant controlled</b>						
24	Online	●				
25	Online capable	●				
26	Offline	●				
<b>Unattended – Cardholder controlled</b>						
34	Online					
35	Online capable					
36	Offline					
<p><b>Legend:</b> ● = Currently applicable combination, Grey boxes indicates combinations not relevant for this specification.</p> <p><sup>1)</sup> = For Cash terminals, Refund transactions are not allowed.</p>						



Table 7.7 – Terminal Types

Terminal Type		Transaction Request		Transaction Type		Terminal Capabilities
<b>Attended – Financial Institution Controlled</b>						
TERM11	Online only	TR00	Purchase	TT01	Cash	All CVMs except No CVM
		TR02	Original Authorisazion	TT01	Cash	All CVMs except No CVM
		TR04	Capture	TT01	Cash	All CVMs except No CVM
<b>Attended – Merchant Controlled</b>						
TERM21	Online only	TR00	Purchase	TT11	Quasi-Cash	All CVMs except No CVM
TERM22	Offline with online Capability	TR00	Purchase	TT00	Goods and Services	All CVMs
		TR01	Refund	TT20	Refunds	Signature only (Merchant)
		TR02	Original Authorization	TT00	Goods and Services	All CVMs
		TR04	Capture	TT00	Goods and Services	All CVMs
		TR05	Reversal	TT00	Goods and Services	–
<b>Unattended – Merchant Controlled</b>						
TERM24	Online only	TR00	Purchase	TT00	Goods and Services	Online PIN only
		TR02	Original Authorisazion	TT00	Goods and Services	Online PIN only
		TR04	Capture	TT00	Goods and Services	Online PIN only
		TR05	Reversal	TT00	Goods and Services	–
TERM25	Offline with online Capability	TR00	Purchase	TT00	Goods and Services	Online PIN & offline PIN
		TR02	Original Authorisazion	TT00	Goods and Services	Online PIN & offline PIN
		TR04	Capture	TT00	Goods and Services	Online PIN & offline PIN
		TR05	Reversal	TT00	Goods and Services	–
TERM25	Offline with online Capability	TR00	Purchase	TT00	Goods and Services	No CVM
TERM26	Offline only	TR00	Purchase	TT00	Goods and Services	No CVM

This page is intentionally left blank

# 8. Commands and Responses

## 8.1 Introduction

This section defines the formats for commands and responses in the terminal.

The detailed definitions of the data elements are given in section 9: “Data Elements”.

## 8.2 Command Overview

Table 8.1 – Command Overview

Application	Command	MT	CLA	INS	Comments
General	Read Magnetic Stripe	'40'	–	–	Defined in ref. 40
	ICC Command	'42'	–	–	Defined in ref. 40
	ICC Power-On	'43'	–	–	Defined in ref. 40
	ICC Power-Off	'44'	–	–	Defined in ref. 40
	ICC Query	'45'	–	–	Defined in ref. 40
	Verify Offline PIN	'46'	–	–	Defined in ref. 40
	Confirm Amount	'60'	–	–	Defined in ref. 40
	Display Message	'61'	–	–	Defined in ref. 40
	Print Message	'63'	–	–	Defined in ref. 40
	Purge Print Buffer	'64'	–	–	Defined in ref. 40
	Get Key Check Value	'65'	–	–	Defined in ref. 40
	Verify PSAM Public Key Certificate	'66'	–	–	Defined in ref. 40
	Get PIN Pad Public Key Record	'67'	–	–	Defined in ref. 40
	Submit Initial Key	'68'	–	–	Defined in ref. 40
	Initiate PIN Entry	'69'	–	–	Defined in ref. 40
	Get PIN	'6A'	–	–	Defined in ref. 40
	Terminate PIN Entry	'6C'	–	–	Defined in ref. 40.
	Get Amount	'80'	–	–	Defined in ref. 40 and section 8.6.23
	Get Amount 2	'80'	–	–	Defined in section 8.6.24, page 8–82
	Get Amount 3	'80'	–	–	Defined in section 8.6.25, page 8–84
	Transaction Completed	'81'	–	–	Defined in ref. 40.
	Funds Available	'82'	–	–	Defined in ref. 40.
	Create File	'90'	–	–	Defined in ref. 40.
	Delete File	'91'	–	–	Defined in ref. 40.
	Add File Record	'92'	–	–	Defined in ref. 40.
	Get File Record	'93'	–	–	Defined in ref. 40.
	Update File Record	'94'	–	–	Defined in ref. 40.
	Find and Get File Record	'95'	–	–	Defined in ref. 40.
	Delete File Record	'96'	–	–	Defined in ref. 40.
	Find and Delete File Record	'97'	–	–	Defined in ref. 40.
	Clear File	'98'	–	–	Defined in ref. 40.
	Initiate Communication Session	'B0'	–	–	Defined in ref. 40.
	Terminate Communication Session	'B1'	–	–	Defined in ref. 40.
	Add Event to Queue	'C0'	–	–	Defined in ref. 40.
Get Event from Queue	'C1'	–	–	Defined in ref. 40.	
Find event on Queue	'C2'	–	–	Defined in ref. 40.	
Flush Event Queue	'C3'	–	–	Defined in ref. 40.	
Open Handler	'F0'	–	–	Defined in ref. 40.	

Table 8.1 – Command overview (*continued*)

Application	Command	MT	CLA	INS	Comments
	Close Handler	'F1'	–	–	Defined in ref. 40.
	Write Handler String	'F3'	–	–	Defined in ref. 40.
	Read Handler String	'F4'	–	–	Defined in ref. 40.
	Get Handler Address	'F5'	–	–	Defined in ref. 40.
<b>Application Selection</b>	Select	'42'	'00'	'A4'	Defined in ref. 36.
	Read Record	'42'	'00'	'B2'	Defined in ref. 36.
<b>Proprietary</b>	Check Stop List	'01'	–	–	Defined in section 8.6.18, page 8–71
	Verify Signature	'02'	–	–	Defined in section 8.6.19, page 8–72
	Verify Local PIN	'03'	–	–	Defined in section 8.7, page 8–86
	Get Merchant Data	'04'	–	–	Defined in section 8.6.20, page 8–74
	Transaction State Information	'05'	–	–	Defined in section 8.6.21, page 8–76
	Repeat Last ICC Response	'06'	–	–	Defined in section 8.6.22, page 8–79
<b>Application Specific (Debit/Credit)</b>					
<b>Administrative</b>	Install	'42'	'B0'	'70'	Defined in section 8.5.1, page 8–21
	Validate Install Data	'42'	'B0'	'7A'	Defined in section 8.5.2, page 8–22
	Add Addendum Record	'42'	'B0'	'72'	Defined in section 8.5.3, page 8–24
	Deactivate PSAM	'42'	'B0'	'74'	Defined in section 8.5.4, page 8–25
	Create Service Record	'42'	'B0'	'76'	Defined in section 8.5.5, page 8–26
	Get Debit/Credit Properties	'42'	'B0'	'A0'	Defined in section 8.5.6, page 8–28
	Set Debit/Credit Properties	'42'	'B0'	'A0'	Defined in section 8.5.7, page 8–32
	PSAM Update	'42'	'B4'	'48'..'4E'	Defined in section 8.5.8, page 8–34
<b>EMV</b>	Initiate EMV Payment	'42'	'B0'	'80'	Defined in section 8.6.1, page 8–35
	Initiate EMV Payment 2 <sup>1)</sup>	'42'	'B0'	'80'	Defined in section 8.6.2, page 8–37
	EMV Payment	'42'	'B0'	'82'	Defined in section 8.6.3, page 8–40
	Validate Data	'42'	'B0'	'84'	Defined in section 8.6.4, page 8–41
	Validate Data 2 <sup>2)</sup>	'42'	'B0'	'84'	Defined in section 8.6.5, page 8–44
	Complete Payment	'42'	'B0'	'8E'	Defined in section 8.6.6, page 8–48
<b>MSC</b>	Initiate MSC Payment	'42'	'B0'	'80'	Defined in section 8.6.7, page 8–49
	Initiate MSC Payment 2 <sup>1)</sup>	'42'	'B0'	'80'	Defined in section 8.6.8, page 8–51
	MSC Payment	'42'	'B0'	'82'	Defined in section 8.6.9, page 8–54
	Validate Data	'42'	'B0'	'84'	Defined in section 8.6.4, page 8–41
	Validate Data 2 <sup>2)</sup>	'42'	'B0'	'84'	Defined in section 8.6.5, page 8–44
	Complete Payment	'42'	'B0'	'8E'	Defined in section 8.6.10, page 8–56
<b>Key Entered</b>	Initiate Key Entered Payment	'42'	'B0'	'80'	Defined in section 8.6.11, page 8–57
	Key Entered Payment	'42'	'B0'	'82'	Defined in section 8.6.12, page 8–60
	Validate Data	'42'	'B0'	'84'	Defined in section 8.6.4, page 8–41
	Validate Data 2 <sup>2)</sup>	'42'	'B0'	'84'	Defined in section 8.6.5, page 8–44
	Complete Payment	'42'	'B0'	'8E'	Defined in section 8.6.13, page 8–62

Table 8.1 – Command overview (*concluded*)

Application	Command	MT	CLA	INS	Comments
<b>Token based</b>	Initiate Token Based Payment	'42'	'B0'	'80'	Defined in section 8.6.14, page 8–64
	Initiate Token Based Payment 2 <sup>1)</sup>	'42'	'B0'	'80'	Defined in section 8.6.15, page 8–65
	Token Based Payment	'42'	'B0'	'84'	Defined in section 8.6.16, page 8–68
	Validate Data	'42'	'B0'	'84'	Defined in section 8.6.4, page 8–41
	Validate Data 2 <sup>2)</sup>	'42'	'B0'	'84'	Defined in section 8.6.5, page 8–44
	Complete Payment	'42'	'B0'	'8E'	Defined in section 8.6.17, page 8–70
<b>PSAM Initialization (Generic)</b>					
	Start-up PSAM	'42'	'B0'	'02'	Defined in section 8.4.1, page 8–9
	PSAM Shutdown	'42'	'B0'	'04'	Defined in ref. 40
	Get Supported AIDs	'42'	'B0'	'08'	Defined in section 8.4.2, page 8–10
	Synchronize PSAM/PIN Pad	'42'	'B0'	'C2'	Defined in section 8.4.6, page 8–17
	Get Next	'42'	'B0'	'FC'	Defined in ref. 40
	Response Command	'42'	'B0'	'FE'	Defined in ref. 40
<b>Application Specific PSAM Initialization (Debit/Credit)</b>					
	Get MSC Table	'42'	'B0'	'30'	Defined in section 8.4.3, page 8–12
	Get Debit/Credit File Characteristics	'42'	'B0'	'32'	Defined in section 8.4.4, page 8–14
	Exchange Debit/Credit Static Information	'42'	'B0'	'3C'	Defined in section 8.4.8, page 8–19
	Configure PSAM Application	'42'	'B0'	'3E'	Defined in section 8.4.5, page 8–16
<b>Legend:</b>					
1) Whether the <i>Initiate Payment 2</i> or <i>Initiate Payment</i> command is to be used depends on whether both the terminal and PSAM supports Service Pack No. 2. or not. For further details, see section 11.					
2) Whether the <i>Validate Data 2</i> or <i>Validate Data</i> command is to be used depends on whether both the terminal and PSAM supports Service Pack No. 1. or not. For further details, see section 11.					

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 8.2 – 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 Local PIN	'03'			'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)
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)
Read Record	'42'	'00'	'B2'	'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)
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)
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)
Get Next	'42'	'B0'	'FC'	'00pp' (PSAM)	
Response Command	'42'	'B0'	'FE'	'00pp' (PSAM) '0202' (Processor Card Handler)	Any
PSAM Update	'42'	'B4'	'48/ '4E'	'00pp' (PSAM)	'0100' (MAD–Handler)
ICC Command	'42'			'0202' (Processor card reader)	Any

**Legend:**  
Grey area indicates TAPA defined commands.

Table 8.2 – Command – Handler Overview (*continued*)

Command	MT	CLA	INS	Destination Address	Source Address
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)	'00pp' (PSAM)
Get Processing Options	'42'	'80'	'A8'	'0202' (Processor card reader)	'00pp' (PSAM)
Generate AC	'42'	'80'	'AE'	'0202' (Processor card reader)	'00pp' (PSAM)
Get Data	'42'	'80'	'CA'	'0202' (Processor 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
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
Initiate PIN Entry	'69'			'0301' (PIN Pad)	Any
Get PIN	'6A'			'0301' (PIN Pad)	Any
Terminate PIN Entry	'6C'			'0301' (PIN Pad)	Any
Get Amount	'80'			'0300' (User Interface Handler) '0400' (Merchant Application Handler)	Any
Transaction Completed	'81'			'0400' (Merchant Application)	Any
Funds Available	'82'			'0400' (Merchant Application)	Any
Create File	'90'			'0500' (Data Store Handler)	Any
Delete File	'91'			'0500' (Data Store Handler)	Any
<b>Legend:</b> Grey area indicates TAPA defined commands.					



Table 8.2 – Command – Handler Overview (*concluded*)

Command	MT	CLA	INS	Destination Address	Source Address
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
<b>Legend:</b> Grey area indicates TAPA defined commands.					

## 8.3 Error Responses

### 8.3.1 MAD-Handler Interface to the PSAM

- 8.3.1.1      A      The format of error responses will be according to ref. 40: “TAPA, Application Architecture Specification” and ref. 41: “TAPA, Application Architecture Specification – Errata”.

## 8.4 Commands used during Initialization

The following sections (8.4.1 to 8.4.8) detail the commands and responses between the MAD–Handler and the PSAM used during initialization/power–up.

### 8.4.1 Start–up PSAM

#### Command Message

- 8.4.1.1 A The *Start–up PSAM* command shall conform to the format defined in table 8.3.

Table 8.3 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD–Handler	1
L <sub>DATA</sub>	'0008'	2
CLA	'B0'	1
INS	'02'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'02'	1
ID <sub>THREAD</sub>	Thread Identifier	1
PSAM sub–address	'pp' – sub–address at which the PSAM is located	1
L <sub>e</sub>	'00'	1

#### Response Message

A *successful* response to the *Start–up PSAM* command has the format defined in table 8.4.

- 8.4.1.2 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 8.4 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0011'	2
PSAM Identification	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>	13
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

## 8.4.2 Get Supported AIDs

### Command Message

- 8.4.2.1 A The *Get Supported AIDs* command shall conform to the format defined in table 8.5.

Table 8.5 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0007'	2
CLA	'B0'	1
INS	'08'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'01'	1
ID <sub>THREAD</sub>	Thread Identifier	1
L <sub>e</sub>	'00'	1

## Response Message

A *successful* response to the *Get Supported AIDs* command has the format defined in table 8.6.

Table 8.6 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
CNT <sub>AID</sub>	Number of AIDs listed in this response The following fields (subscripted by "N") are repeated CNT <sub>AID</sub> times (N = 1 to CNT <sub>AID</sub> )	1
LEN <sub>AIDN</sub>	Length of Nth AID	1
AID <sub>N</sub>	Nth AID	5 – 16
ID <sub>SCHEME, N</sub>	A reference number assigned to AID N by the acquirer	1
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

### 8.4.3 Get MSC Table

#### Command Message

- 8.4.3.1 A The *Get MSC Table* command shall conform to the format defined in table 8.7.

Table 8.7 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0008'	2
CLA	'B0'	1
INS	'30'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'02'	1
ID <sub>THREAD</sub>	Thread Identifier	1
Start Location	'00' = Start at first MSC Table entry '01' = Start at next MSC Table entry	1
L <sub>e</sub>	'00'	1

#### Response Message

A *successful* response to the *Get MSC Table* command has the format defined in table 8.8.

Table 8.8 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
CNT <sub>MSC</sub>	Number of MSC records in this response. The following fields (indicated as MSC record) are repeated CNT <sub>MSC</sub> times.	2
MSC record		
PAN <sub>FROM</sub>	PAN range from	4
PAN <sub>TO</sub>	PAN range to	4
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

## 8.4.4 Get Debit/Credit File Characteristics

### Command Message

- 8.4.4.1 A The *Get Debit/Credit File Characteristics* command shall conform to the format defined in table 8.9.

Table 8.9 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0007'	2
CLA	'B0'	1
INS	'32'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'01'	1
ID <sub>THREAD</sub>	Thread Identifier	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Get Debit/Credit File Characteristics* command has the format defined in table 8.10.



Table 8.10 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0018'	2
Administrative File		
NUM <sub>FILE</sub>	Number of files. '00' or '01' depending on whether or not the PSAM uses an Administrative File	1
LEN <sub>KEY</sub>	Length of search key ('00' if no search key is used)	1
LEN <sub>REC</sub>	Maximum record length (in bytes) required	2
Priority1 Files		
NUM <sub>FILE</sub>	'01' ('00' if priority1 File is not used)	1
LEN <sub>KEY</sub>	Length of search key ('00' if no search key is used)	1
LEN <sub>REC</sub>	Maximum record length (in bytes) required	2
Priority2 Files		
NUM <sub>FILE</sub>	'01' ('00' if priority2 File is not used)	1
LEN <sub>KEY</sub>	Length of search key ('00' if no search key is used)	1
LEN <sub>REC</sub>	Maximum record length (in bytes) required	2
Priority3 Files		
NUM <sub>FILE</sub>	'01' ('00' if priority3 File is not used)	1
LEN <sub>KEY</sub>	Length of search key ('00' if no search key is used)	1
LEN <sub>REC</sub>	Maximum record length (in bytes) required	2
Priority4 Files		
NUM <sub>FILE</sub>	'01' ('00' if priority4 File is not used)	1
LEN <sub>KEY</sub>	Length of search key ('00' if no search key is used)	1
LEN <sub>REC</sub>	Maximum record length (in bytes) required	2
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.4.5 Configure PSAM Application

### Command Message

- 8.4.5.1 A The *Configure PSAM Application* command shall conform to the format defined in table 8.11.

Table 8.11 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'3E'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier	1
FILEID <sub>ADMIN</sub>	File identifier for the administrative file Will be zeroes if the administrative file is not used.	2
FILEID <sub>PRIORITY,n</sub>	A list of file identifiers for the priority files	2*n
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Configure PSAM Application* command has the format defined in table 8.12.

Table 8.12 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

## 8.4.6 Synchronize PSAM/PIN Pad

### Command Message

- 8.4.6.1 A The *Synchronize PSAM/PIN Pad* command shall conform to the format defined in table 8.13.

Table 8.13 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0007'	2
CLA	'B0'	1
INS	'C2'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'01'	1
ID <sub>THREAD</sub>	Thread Identifier	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Synchronize PSAM/PIN Pad* command has the format defined in table 8.14.

Table 8.14 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'000C'	2
PIN Pad Identifier		
ID <sub>PPCREATOR</sub>	Unique ID of PIN Pad Creator	4
ID <sub>PP</sub>	Unique ID of PIN Pad	4
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.4.7 Get Next

### Command Message

- 8.4.7.1 A The *Get Next* command shall conform to the format defined in table 8.15.

Table 8.15 – Command message for the *Get Next* command

Field	Value	Length (bytes)
CLA	'B0'	1
INS	'FC'	1
P1	ID <sub>THREAD</sub>	1
P2	'00'	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Get Next* command has the format defined in table 8.16.

Table 8.16 – 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 8.17.

Table 8.17 – 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 <i>Get Next</i> command to get the remaining Response Data

## 8.4.8 Exchange Debit/Credit Static Information

### Command Message

- 8.4.8.1 A The *Exchange Debit/Credit Static Information* command shall have the format shown in table 8.18.

Table 8.18 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0025'	2
CLA	'B0'	1
INS	'3C'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'1F'	1
ID <sub>THREAD</sub>	Thread Identifier	1
Terminal Capabilities	Terminal Capabilities according to ref. 36: "EMV, version 4.1"	3
Additional Terminal Capabilities	Additional Terminal Capabilities according to ref. 36: "EMV, version 4.1"	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. 36: "EMV, version 4.1"	1
POS Capability Code	Point of Sale Capability Code. See section F.9.4.	6
Info Level	Merchant Application Log requested or not & PSAM State Information send to Merchant Application or not.	1
L <sub>e</sub>	'00'	1

### Response Message

A successful response to the *Exchange Debit/Credit Static Information* command has the format shown in table 8.19.

- 8.4.8.2 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 8.19 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	‘0071’	2
Signature Verification	‘00’ = Signature verification by merchant is not required ‘FF’ = Signature verification by merchant is required	1
CNT <sub>ENTRIES</sub>	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 <sub>NUMBER</sub>	Merchant No. assigned by PBS	5
ME <sub>NAME</sub>	Merchant Name	18
ME <sub>CITY</sub>	Merchant City Name	16
ME <sub>ADDRESS</sub>	Merchant Address	24
ME <sub>ZIP</sub>	Merchant Postal Code	8
ME <sub>PHONE</sub>	Merchant Phone No.	24
ME <sub>BRN</sub>	Merchant Business Registration Number (CVR–Number)	12
ASW1–ASW2	Application Status Words	2
RC	‘0000’	2

## 8.5 Debit/Credit Administrative Commands

### 8.5.1 Install

#### Command Message

8.5.1.1 A The *Install* command shall have the format shown in table 8.20.

Table 8.20 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0025'	2
CLA	'B0'	1
INS	'70'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'1F'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Terminal Capabilities	Terminal Capabilities according to ref. 36: "EMV, version 4.1"	3
Additional Terminal Capabilities	Additional Terminal Capabilities according to ref. 36: "EMV, version 4.1"	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. 36: "EMV, version 4.1"	1
POS Capability Code	Point of Sale Capability Code. See section F.9.4.	6
Info Level	Merchant Application Log requested or not & PSAM State Information send to Merchant Application or not.	1
L <sub>e</sub>	'00'	1

#### Response Message

A *successful* response to the *Install* command has the format shown in table 8.21.

Table 8.21 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>HREQ</sub>	Length of host request (Install)	2
Host Request	Host request message	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

## 8.5.2 Validate Install Data

### Command Message

- 8.5.2.1 A The *Validate Install Data* command shall have the format shown in table 8.44.

Table 8.22 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'7A'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
LEN <sub>HR</sub>	Length of host data (if no online connection then equal to '00')	2
Host Response	Host response data	Variable
L <sub>e</sub>	'00'	1



## Response Message

A *successful* response to the *Validate Install Data* command has the format shown in table 8.46.

Table 8.23 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

### 8.5.3 Add Addendum Record

#### Command Message

- 8.5.3.1 A The *Add Addendum Record* command shall have the format shown in table 8.24.

Table 8.24 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'72'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Addendum Status	MSB: Segment number of this Addendum Record LSB: Total number of segments	2
LEN <sub>PAN</sub>	Length of the Primary Account Number	1
PAN	The Primary Account Number	Up to 10
<b>Original Data Elements</b>		
STAN	Systems Trace Audit Number	3
Time	Time, local transaction	3
Date	Date, local transaction	2
MRC	Message Reason Code (see Attachment F, section F.9.7)	2
Batch Number	Batch Number used for reconciliation	12
Terminal ident.	Terminal Identification (according to ref. 36: "EMV Version 4.1")	8
MAD-Handler ID	Unique identifier of the terminal equipment	8
Terminal Approval No.	Unique number identifying a certified terminal	2
LEN <sub>ADD</sub>	Length of the addendum record	2
Addendum Record	Addendum record to be linked to a previous financial transaction	Variable
L <sub>e</sub>	'00'	1

## Response Message

A *successful* response to the *Add Addendum Record* command has the format shown in table 8.25.

Table 8.25 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.5.4 Deactivate PSAM

### Command Message

8.5.4.1 A The *Deactivate PSAM* command shall have the format shown in table 8.26.

Table 8.26 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD–Handler	1
L <sub>DATA</sub>	'0011'	2
CLA	'B0'	1
INS	'74'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'0B'	1
ID <sub>THREAD</sub>	'00'	1
Terminal Approval No.	Unique number identifying a certified Terminal	2
MAD–Handler ID	Unique number identifying a certified terminal	8
L <sub>e</sub>	'00'	1

## Response Message

A *successful* response to the *Deactivate PSAM* command has the format shown in table 8.27.

Table 8.27 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>HREQ</sub>	Length of host request (Deactivate)	2
Host Request	Host request message	Variable
ASW1-ASW2	Application Status Words	2
RC	'0000'	2

## 8.5.5 Create Service Record

### Command Message

- 8.5.5.1 A The *Create Service Record* command shall have the format shown in table 8.28.

Table 8.28 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0007'	2
CLA	'B0'	1
INS	'76'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'01'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>e</sub>	'00'	1

## Response Message

A *successful* response to the *Create Service Record* command has the format shown in table 8.29.

Table 8.29 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.5.6 Get Debit/Credit Properties

### Command Message

- 8.5.6.1 A The *Get Debit/Credit Properties* command shall have the format shown in table 8.30.

Table 8.30 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'A0'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Identifier	Identifies the Property / data element to be requested (see table 8.32)	2
LEN <sub>INFO</sub>	Length of the Additional Info ('00' if absent)	1
Additional Info	Present if additional information is required (see table 8.32)	Variable
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Get Debit/Credit Properties* command has the format shown in table 8.31.

Table 8.31 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>PROPERTY</sub>	Length of the properties requested ('0000' if absent)	2
Property	Property / Data element (see table 8.32)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

Table 8.32 – 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 <sub>TRACK2</sub>	1	Card Name	16
		Track2 Data	Up to 19	Card Service Info	1
				Service Code	0 or 2 <sup>1)</sup>
'0003'	Additional PSAM Info	(Empty)	0	PSAM Identifier <sup>2)</sup>	13
				PSAM Version	1
				PSAM Subversion	1
				PSAM D/C Life Cycle State	1
				Service Packs supported	1
				LEN <sub>DD</sub> (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 <sub>PAN</sub> <sup>3)</sup>	1	Reference STAN	3
		PAN <sup>4)</sup>	Up to 10	Amount	4
				CURRC	2
				CURRE	1
				DTHR	5



Table 8.32 – Properties / Data Elements to be Requested (*concluded*)

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) <sup>5)</sup>	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 <sub>Terminal Checksum</sub>	1 <sup>6)</sup>	EMV Checksum	8
		Terminal Checksum	up to 200	PSAM Code Checksum	8
				PSAM Config Checksum	8
'0008'	Envelope buffer size	(Empty)	0	Max. length (bytes) of envelope data for MSC transactions	1
				Max. length (bytes) of envelope data for EMV transactions	1
'0009' – '7FFF'	Reserved for Future Use				
<p><b>Legend:</b></p> <p>The coding of the data elements can be found in section 9, "Data Elements".</p> <p>1) Omitted if not accessible.</p> <p>2) PSAM Identifier consist of RID<sub>PSAM</sub>    ID<sub>PSAMCREATOR</sub>    ID<sub>PSAM</sub>.</p> <p>3) Number of bytes (in case of odd number of digits, the PAN shall be padded with a trailing 'F')</p> <p>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.</p> <p>5) The index indicates to which key chain the information are associated.</p> <p>6) Terminal Checksum shall be in the range 4 – 20 bytes.</p>					

8.5.6.2 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.

## 8.5.7 Set Debit/Credit Properties

### Command Message

8.5.7.1 A The *Set Debit/Credit Properties* command shall have the format shown in table 8.33.

Table 8.33 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'A0'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>C</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Identifier	Identifies the Property / data element to be requested (see table 8.35)	2
LEN <sub>INFO</sub>	Length of the Additional Info ('00' if absent)	1
Additional Info	Present if additional information is required (see table 8.35)	Variable
L <sub>e</sub>	'00'	1

**NOTE:** If the Additional Info contains a length field, LEN<sub>INFO</sub> shall include this field even

### Response Message

A *successful* response to the *Set Debit/Credit Properties* command has the format shown in table 8.34.

Table 8.34 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>PROPERTY</sub>	Length of the properties requested ('0000' if absent)	2
Property	Property / Data element (see table 8.35)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

Table 8.35 – 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 <sub>I</sub> ED	1 <sup>1)</sup>	(Empty)	0
		Issuer Envelope Data	0 – 150 <sup>2)</sup>		
'8001'	Terminal Settings	Terminal Settings	1		
'8002'	Duplicate Transaction Time–out	Duplicate Transaction Time–out	1		
'8003' – '8FFF'	Reserved for Future Use				
<b>Legend:</b>					
The coding of the data elements can be found in section 9, "Data Elements".					
1) LEN <sub>I</sub> ED = '00' will reset the Issuer Envelope Data.					
2) The maximum length of the Issuer Envelope Data is currently limited to 60 bytes for EMV transactions and 150 bytes for MSC transactions.					

## 8.5.8 PSAM Update

### Command Message

- 8.5.8.1 A The *PSAM Update* command shall have the format shown in table 8.36.

Table 8.36 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B4'	1
INS	'48' = Clear Data '4A' = Reserved for Future Use '4C' = Encrypted Data (e.g. code updates) '4E' = Encrypted Keys	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111' or '0011'	2
L <sub>C</sub>	Variable	1
ID <sub>THREAD</sub>	'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 <sub>UPD</sub>	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 <sub>UPD</sub> . The data bytes included may be padded to reach a multiple of 8 bytes.	Variable
S <sub>UPD</sub>	MAC over the whole command (CLA – Update Data)	8
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *PSAM Update* command has the format shown in table 8.37.

Table 8.37 – Successful response message for the *PSAM Update* 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6 Debit/Credit Transaction Commands

The following sections (8.6.1 to 8.6.21) detail the commands and responses between the MAD–Handler, PSAM and Merchant Application used during debit/credit transactions.

### 8.6.1 Initiate EMV Payment

#### Command Message

- 8.6.1.1 A The *Initiate EMV Payment* command shall have the format shown in table 8.38.

Table 8.38 – Command message of the *Initiate 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – 'FF' = Reserved for future use	1
LEN <sub>AID</sub>	Length of AID	1
AID <sub>EMV</sub>	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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>FCI</sub>	Length of FCI (starting with '6F' (FCI template))	1
FCI	File Control Information conveyed in the Select response	Variable
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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
L <sub>e</sub>	'00'	1

## Response Message

A successful response to the *Initiate EMV Payment* command has the format shown in table 8.39.

Table 8.39 – Successful response message for the *Initiate 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
DATE <sub>EFFECTIVE</sub>	Application Effective Date	3
PAN <sub>SEQUENCE</sub>	Application PAN Sequence Number	1
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.2 Initiate EMV Payment 2

- 8.6.2.1 A This command/response format shall be used if both the terminal and PSAM supports Service Pack. No. 2. For further details, see section 11, "Service Packs".

### Command Message

- 8.6.2.2 A The *Initiate EMV Payment 2* command shall have the format shown in table 8.40.

Table 8.40 – Command message of the *Initiate EMV 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – 'FF' = Reserved for future use	1
LEN <sub>AID</sub>	Length of AID	1
AID <sub>EMV</sub>	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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>FCI</sub>	Length of FCI (starting with '6F' (FCI template))	1
FCI	File Control Information conveyed in the Select response	Variable
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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 <sub>e</sub>	'00'	1



## Response Message

A *successful* response to the *Initiate EMV Payment 2* command has the format shown in table 8.41.

Table 8.41 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
DATE <sub>EFFECTIVE</sub>	Application Effective Date	3
PAN <sub>SEQUENCE</sub>	Application PAN Sequence Number	1
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

### 8.6.3 EMV Payment

#### Command Message

- 8.6.3.1 A The *EMV Payment* command shall have the format shown in table 8.42.

Table 8.42 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN <sub>MDOL1</sub>	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 <sub>e</sub>	'00'	1

#### Response Message

A *successful* response to the *EMV Payment* command has the format shown in table 8.43.

Table 8.43 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
ATC	Application Transaction Counter (ATC)	2
LEN <sub>HREQ</sub>	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN <sub>MDOL2</sub>	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.4 Validate Data

### Command Message

- 8.6.4.1 A The *Validate Data* command shall have the format shown in table 8.44.
- 8.6.4.2 A If the L<sub>C</sub> field exceeds 248 bytes, the MAD–Handler shall deliver the data in two command APDUs (segments).
- 8.6.4.3 A In such a command the MAD–Handler shall send first L<sub>C</sub> = 248 bytes of data in the first segment.

Table 8.44 – Command message of the *Validate 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'84'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	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 <sub>MDOL2</sub> <sup>1)</sup>	Length of the concatenated list of data elements (MDOL2 data)	1
MDOL2 Data <sup>1)</sup>	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 <sub>HR</sub> <sup>1)</sup>	Length of host data (if no online connection then equal to '0000')	2
Host Response <sup>1)</sup>	Host response data	Variable
L <sub>e</sub>	'00'	1

- <sup>1)</sup> The first (248 – 2 (ID<sub>THREAD</sub> & Segment Number)) bytes are conveyed in the first segment (segment number 1).

**NOTE:** If LEN<sub>MDOL2</sub> is the maximum value of 255 bytes, the Host Response is limited to:  

$$246 * 2 - (\text{MDOL2 Data}_{\text{MAX}} + \text{LEN}_{\text{MDOL2}} + \text{LEN}_{\text{HR}})$$

$$= 246 * 2 - (255 + 1 + 2) = 234 \text{ bytes}$$

**NOTE:** See example of the Application Chaining in figure 8.1 on page 8-46

### Response Message

A *successful* response to the *Validate Data* command has the format shown in table 8.45 and 8.46, depending of the segment number.

Table 8.45 – Successful response message for the *Validate Data* 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1–ASW2	'0000'	2
RC	'0000'	2

Table 8.46 – Successful response message for the *Validate Data* 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Action Code	Action Code from the acquirer/PSAM	2
LEN <sub>STAN+HREQ</sub>	Length of STAN and host request ('0000' if absent) <sup>1)</sup>	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.

### Error Response

Both “short” error responses (as defined in section 8.3) or “full–size” responses (according to table 8.46) may be returned, when the value of ASW1–ASW2 is greater than or equal to '11 00'.

## 8.6.5 Validate Data 2

- 8.6.5.1 A This command/response format shall be used if both the terminal and PSAM supports Service Pack. No. 1. For further details, see section 11, “Service Packs”.

### Command Message

- 8.6.5.2 A The *Validate Data 2* command shall have the format shown in table 8.47.
- 8.6.5.3 A If the  $L_C$  field exceeds 248 bytes, the MAD-Handler shall deliver the data in two command APDUs (segments).
- 8.6.5.4 A In such a command the MAD-Handler shall send first  $L_C = 248$  bytes of data in the first segment.

Table 8.47 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'84'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	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 <sub>MDOL2</sub> <sup>1)</sup>	Length of the concatenated list of data elements (MDOL2 data)	1
MDOL2 Data <sup>1)</sup>	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 <sub>HR</sub> <sup>1)</sup>	Length of host data (if no online connection then equal to '0000')	2
Host Response <sup>1)</sup>	Host response data	Variable
L <sub>e</sub>	'00'	1

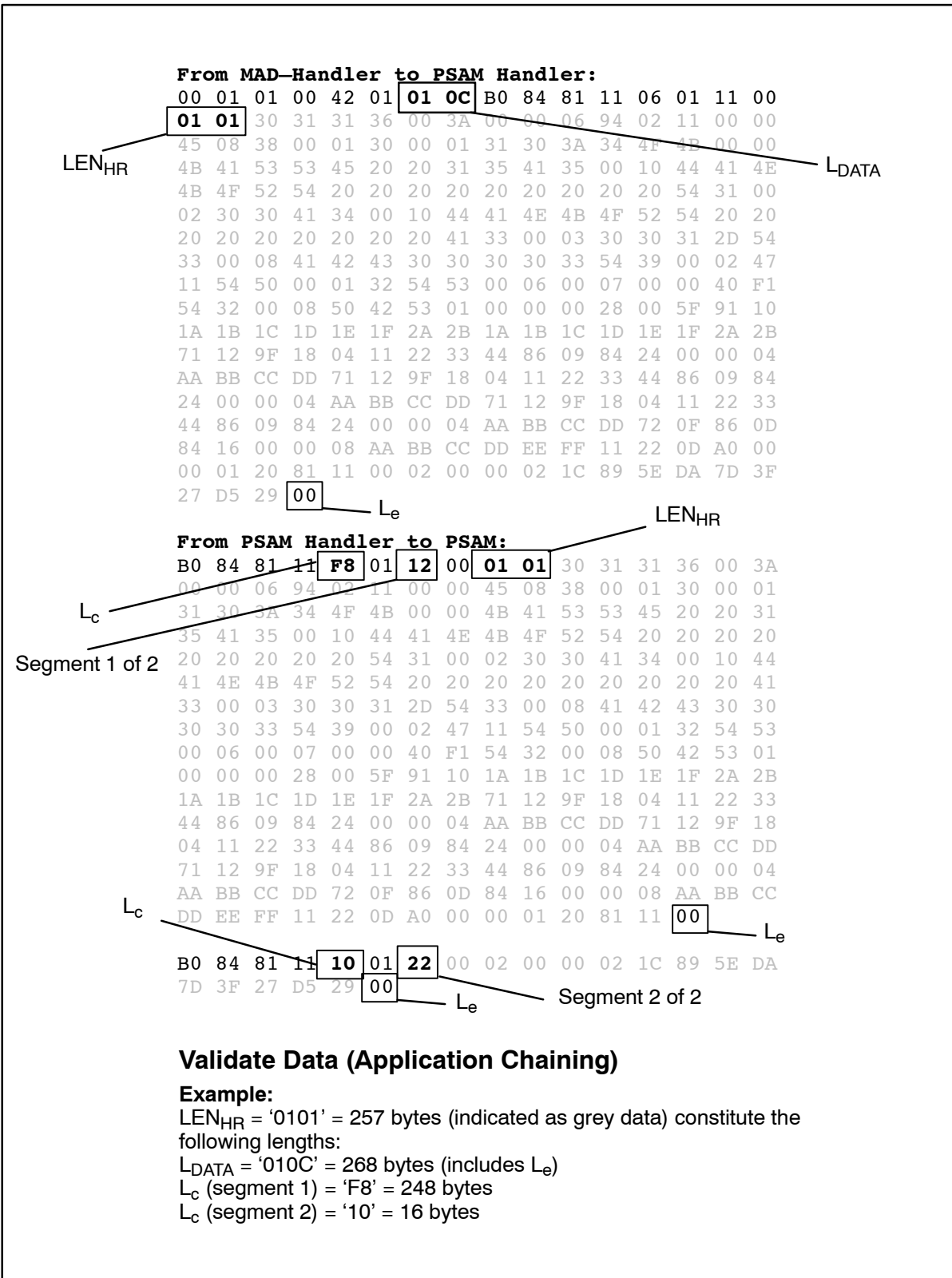
<sup>1)</sup> The first (248 – 2 (ID<sub>THREAD</sub> & Segment Number)) bytes are conveyed in the first segment (segment number 1).

**NOTE:** If  $LEN_{MDOL2}$  is the maximum value of 255 bytes, the Host Response is limited to:

$$246 * 2 - (MDOL2 Data_{MAX} + LEN_{MDOL2} + LEN_{HR}) \\ = 246 * 2 - (255 + 1 + 2) = 234 \text{ bytes}$$

**NOTE:** See example of the Application Chaining in figure 8.1 on page 8–46

Figure 8.1 – Validate Data Command – Application Chaining (Example)



**Response Message**

A successful response to the *Validate Data 2* command has the format shown in table 8.48 and 8.49, depending of the segment number.



Table 8.48 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0004'	2
ASW1–ASW2	'0000'	2
RC	'0000'	2

Table 8.49 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Action Code–dePRINT	Action Code from the acquirer/PSAM	2
Approval Code	Approval Code/Authorisation Code (filled with zeroes if absent) <sup>5)</sup>	6
ARC	Authorization Response Code <sup>2)</sup> ('0000' if absent)	2
POS Entry Mode	Source of cardholder account data <sup>3)</sup>	3
CVM Status	Type of CVM and authorization <sup>4)</sup>	1
LEN <sub>STAN+HREQ</sub>	Length of STAN and host request ('0000' if absent) <sup>1)</sup>	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.

### Error Response

Both “short” error responses (as defined in section 8.3) or “full-size” responses (according to table 8.49) may be returned, when the value of ASW1–ASW2 is greater than or equal to '11 00'.

## 8.6.6 Complete Payment

### Command Message

- 8.6.6.1 A The *Complete Payment* command shall have the format shown in table 8.50.

Table 8.50 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'02'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	<p><b>'00' – '7F' = Successful</b>            '00' = Successful transaction            '01' = Signature accepted            '02' – '7F' = Reserved for Future Use</p> <p><b>'80' – 'FF' = Declined</b>            '80' = Transaction aborted by merchant/cardholder            '81' = Signature rejected            '82' = Goods or services not delivered            '83' – 'FF' = Reserved for Future Use</p>	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 8.51.

Table 8.51 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>TOKEN</sub>	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

## 8.6.7 Initiate MSC Payment

### Command Message

- 8.6.7.1 A The *Initiate MSC Payment* command shall have the format shown in table 8.52.

Table 8.52 – Command message of the *Initiate 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – '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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>TRACK2</sub>	Length of track2	1
TRACK2 DATA	Card data according to POS Entry Mode	Up to 19
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Initiate MSC Payment* command has the format shown in table 8.53.

Table 8.53 – Successful response message for the *Initiate 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

### 8.6.8 Initiate MSC Payment 2

- 8.6.8.1 A This command/response format shall be used if both the terminal and PSAM supports Service Pack. No. 2. For further details, see section 11, "Service Packs".

#### Command Message

- 8.6.8.2 A The *Initiate MSC Payment 2* command shall have the format shown in table 8.54.

Table 8.54 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – '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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>TRACK2</sub>	Length of track2	1
TRACK2 DATA	Card data according to POS Entry Mode	Up to 19
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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 <sub>e</sub>	'00'	1

## Response Message

A *successful* response to the *Initiate MSC Payment 2* command has the format shown in table 8.55.

Table 8.55 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.9 MSC Payment

### Command Message

- 8.6.9.1 A The *MSC Payment* command shall have the format shown in table 8.56.

Table 8.56 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN <sub>MDOL1</sub>	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 <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *MSC Payment* command has the format shown in table 8.57.



Table 8.57 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
LEN <sub>HREQ</sub>	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN <sub>MDOL2</sub>	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.10 Complete Payment

### Command Message

8.6.10.1 A The *Complete Payment* command shall have the format shown in table 8.58.

Table 8.58 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'02'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	<p><b>'00' – '7F' = Successful</b>            '00' = Successful transaction            '01' = Signature accepted            '02' – '7F' = Reserved for Future Use</p> <p><b>'80' – 'FF' = Declined</b>            '80' = Transaction aborted by merchant/cardholder            '81' = Signature rejected            '82' = Goods or services not delivered            '83' – 'FF' = Reserved for Future Use</p>	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 8.59.

Table 8.59 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>TOKEN</sub>	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

### 8.6.11 Initiate Key Entered Payment

#### Command Message

- 8.6.11.1 A The *Initiate Key Entered Payment* command shall have the format shown in table 8.60.

Table 8.60 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – '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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data, e.g. key-entered	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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
L <sub>e</sub>	'00'	1

### Response Message

A successful response to the *Initiate Key Entered Payment* command has the format shown in table 8.61.

Table 8.61 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.12 Key Entered Payment

### Command Message

- 8.6.12.1 A The *Key Entered Payment* command shall have the format shown in table 8.62.

Table 8.62 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN <sub>MDOL1</sub>	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 <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Key Entered Payment* command has the format shown in table 8.63.

Table 8.63 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
LEN <sub>HREQ</sub>	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN <sub>MDOL2</sub>	Length of MDOL2 ('00' if absent)	1
MDOL2	MAD Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.13 Complete Payment

### Command Message

- 8.6.13.1 A The *Complete Payment* command shall have the format shown in table 8.64.

Table 8.64 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'02'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	<p><b>'00' – '7F' = Successful</b>            '00' = Successful transaction            '01' = Signature accepted            '02' – '7F' = Reserved for Future Use</p> <p><b>'80' – 'FF' = Declined</b>            '80' = Transaction aborted by merchant/cardholder            '81' = Signature rejected            '82' = Goods or services not delivered            '83' – 'FF' = Reserved for Future Use</p>	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 8.65.



Table 8.65 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>TOKEN</sub>	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

## 8.6.14 Initiate Token Based Payment

### Command Message

- 8.6.14.1 A The *Initiate Token Based Payment* command shall have the format shown in table 8.66.

Table 8.66 – Command message of the *Initiate 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>C</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – '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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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
L <sub>e</sub>	'00'	1

## Response Message

A *successful* response to the *Initiate Token Based Payment* command has the format shown in table 8.67.

Table 8.67 – Successful response message for the *Initiate 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
LEN <sub>EMV</sub>	Length of EMV related data ('00' if absent)	1
DATE <sub>EFFECT.</sub>	Application Effective Date	3
PAN <sub>SEQUENCE</sub>	Application PAN Sequence Number	1
AID <sub>EMV</sub>	AID of the selected application	5 – 16
ME <sub>NUMBER</sub>	Merchant Number	5
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

### 8.6.15 Initiate Token Based Payment 2

- 8.6.15.1 A This command/response format shall be used if both the terminal and PSAM supports Service Pack. No. 2. For further details, see section 11, "Service Packs".

#### Command Message

- 8.6.15.2 A The *Initiate Token Based Payment* command shall have the format shown in table 8.68.

Table 8.68 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Card Data Source	'00' = EMV, '01' = MSC, '02' = Key entered, '03' = Token '04' – '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. 36: "EMV, version 4.1")	8
POS Entry Mode	Source of cardholder account data	3
TT	Transaction Type (according to ref. 36: "EMV, version 4.1")	1
LEN <sub>STAT</sub>	Length of statistics ('00' if absent)	1
Statistics	Statistics of the behavior of the terminal	Variable
LEN <sub>AMOUNTS</sub>	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 <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Initiate Token Based Payment 2* command has the format shown in table 8.69.

Table 8.69 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Card Name	Card official name (coded according to ref. 15: "ISO 8859–15")	16
STAN	Systems Trace Audit Number	3
LEN <sub>EMV</sub>	Length of EMV related data ('00' if absent)	1
DATE <sub>EFFECT.</sub>	Application Effective Date	3
PAN <sub>SEQUENCE</sub>	Application PAN Sequence Number	1
AID <sub>EMV</sub>	AID of the selected application	5 – 16
ME <sub>NUMBER</sub>	Merchant Number	5
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	The Primary Account Number	Up to 10
LEN <sub>MDOL1</sub>	Length of MDOL1 ('00' if absent)	1
MDOL1	MAD–Handler Data Object List (optional)	Variable
ASW1–ASW2	Application Status Words	2
RC	'0000'	2

## 8.6.16 Token Based Payment

### Command Message

8.6.16.1 A The *Token Based Payment* command shall have the format shown in table 8.70.

Table 8.70 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	Variable	2
CLA	'B0'	1
INS	'82'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	Variable	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Batch Number	Batch Number used for reconciliation	12
LEN <sub>MDOL1</sub>	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 <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Token Based Payment* command has the format shown in table 8.71.

Table 8.71 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
CVM Status	Signature required or not, PIN verification performed or not	1
ATC	Application Transaction Counter (ATC)	2
LEN <sub>HREQ</sub>	Length of host request ('0000' if absent)	2
Host Request	Host request message	Variable
LEN <sub>MDOL2</sub>	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.

## 8.6.17 Complete Payment

### Command Message

8.6.17.1 A The *Complete Payment* command shall have the format shown in table 8.72.

Table 8.72 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0008'	2
CLA	'B0'	1
INS	'8E'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'02'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
Transaction Status	<p><b>'00' – '7F' = Successful</b>            '00' = Successful transaction            '01' = Signature accepted            '02' – '7F' = Reserved for Future Use</p> <p><b>'80' – 'FF' = Declined</b>            '80' = Transaction aborted by merchant/cardholder            '81' = Signature rejected            '82' = Goods or services not delivered            '83' – 'FF' = Reserved for Future Use</p>	1
L <sub>e</sub>	'00'	1

### Response Message

A *successful* response to the *Complete Payment* command has the format shown in table 8.73.



Table 8.73 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
LEN <sub>TOKEN</sub>	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

### 8.6.18 Check Stop List

#### Command Message

The *Check Stop List* command has the format shown in table 8.74.

Table 8.74 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD–Handler	1
L <sub>DATA</sub>	Variable	2
LEN <sub>PAN</sub>	Length of the Primary Account Number	1
PAN	The Primary Account Number	Up to 10

#### Response Message

- 8.6.18.1 A A *successful* response to the *Check Stop List* command shall have the format shown in table 8.75.

Table 8.75 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0009'	2
Stop List Status	'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' = Reserved for Future Use '80' = Voice Authorization rejected '81' – 'FF' = Reserved for Future Use	1
Approval Code	Approval Code/Authorisation Code. If absent filled with spaces (format, see Attachment F)	6
RC	'0000'	2

### Response Codes

The Response Codes (RCs) applicable for the *Check Stop List* command are defined in table 8.76.

Table 8.76 – 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

## 8.6.19 Verify Signature

### Command Message

- 8.6.19.1 C The *Verify Signature* command shall have the format shown in table 8.77.

Table 8.77 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD–Handler	1
L <sub>DATA</sub>	'0000'	2

### Response Message

- 8.6.19.2 C A *successful* response to the *Verify Signature* command shall have the format shown in table 8.78.

Table 8.78 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'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 8.79.

Table 8.79 – 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

## 8.6.20 Get Merchant Data

### Command Message

The *Get Merchant Data* command has the format shown in table 8.80.

Table 8.80 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0001'	2
Data Requested	'00' = Token related data '01' = Key Entered Data (PAN    Expiry Date    CV-2) '02' – 'FF' = Reserved for Future Use	1

### Response Message

- 8.6.20.1 A A *successful* response to the *Get Merchant Data* (Token related data is requested) command shall have the format shown in table 8.81.
- 8.6.20.2 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 8.81 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Data Requested	'00' = Token related data	1
LEN <sub>DATA</sub>	Length of Token related data	2
Token Data	Token related data	Variable
RC	'0000'	2

8.6.20.3 A A *successful* response to the *Get Merchant Data* (Key entered data is requested) command shall have the format shown in table 8.82.

Table 8.82 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	Variable	2
Data Requested	'01' = Key Entered Data	1
LEN <sub>CARDDATA</sub>	Length of key entered data	1
Card Data	PAN    Expiry Date    CV-2	Up to 14
RC	'0000'	2

### Response Codes

The Response Codes (RCs) applicable for the *Get Merchant Data* command are defined in table 8.83.

Table 8.83 – 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

## 8.6.21 Transaction State Information

### Command Message

The *Transaction State Information* command has the format shown in table 8.84.

Table 8.84 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'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

- 8.6.21.1 A A *successful* response to the *Transaction State Information* command shall have the format shown in table 8.85.

Table 8.85 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0002'	2
RC	'0000'	2

### Response Codes

The Response Codes (RCs) applicable for the *Transaction State Information* command are defined in table 8.86.

Table 8.86 – Response Codes applicable for the *Transaction State Information* command

<b>RC</b>	<b>Meaning</b>	<b>Usage</b>
'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



## 8.6.22 Repeat Last ICC Response

### Command Message

The *Repeat Last ICC Response* command has the format shown in table 8.87.

Table 8.87 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0000'	2

### Response Message

- 8.6.22.1 A A *successful* response to the *Repeat Last ICC Response* command shall have the format shown in table 8.88.

Table 8.88 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	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<sub>DATA</sub>, 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*.

## 8.6.23 Get Amount

### Command Message

The *Get Amount* command has the format shown in table 8.89.

Table 8.89 – Command message of the *Get Amount* 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'0009'	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	3

### Response Message

- 8.6.23.1 A A *successful* response to the *Get Amount* command shall have the format shown in table 8.90.

Table 8.90 – Successful response message for the *Get Amount* 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0009'	2
Transaction Amount	Transaction Amount	4
CURR	Currency Code and exponent	3
RC	'0000'	2

### Response Codes

The Response Codes (RCs) applicable for the *Get Amount* command are defined in table 8.91.

Table 8.91 – Response Codes applicable for the *Get Amount* 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

## 8.6.24 Get Amount 2

**NOTE:** The *Get Amount 2* command is applicable only if Service Pack No. 1 is mutually supported by the terminal and PSAM. For further details, see section 11.4.2 on page 11-3.

### Command Message

The *Get Amount 2* command has the format shown in table 8.92.

Table 8.92 – Command message of the *Get Amount 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	'80'	1
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'000E'	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	3
LEN <sub>DD</sub>	'0004' Length of Discretionary Data	1
PAN-prefix	8 most significant digits of the PAN	4

### Response Message

- 8.6.24.1 A A *successful* response to the *Get Amount 2* command shall have the format shown in table 8.93.

Table 8.93 – Successful response message for the *Get Amount 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'000F'	2
Transaction Amount	Transaction Amount	4
CURR	Currency Code and exponent	3
LEN <sub>DD</sub>	'0004' Length of Discretionary Data	2
Amount Other	Amount Other ('00 00 00 00' if absent)	4
RC	'0000'	2

### Response Codes

The Response Codes (RCs) applicable for the *Get Amount 2* command are defined in table 8.94.

Table 8.94 – Response Codes applicable for the *Get Amount 2* 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

## 8.6.25 Get Amount 3

**NOTE:** The *Get Amount 3* command is applicable only if Service Pack No. 2 is mutually supported by the terminal and PSAM. For further details, see section 11.5.1 on page 11–5.

### Command Message

The *Get Amount 3* command has the format shown in table 8.95.

Table 8.95 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'000A' + LEN <sub>DD</sub>	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 <sub>DD</sub>	Length of Discretionary Data	1
LEN <sub>PAN</sub>	Length of the Primary Account Number ('00' if absent)	1
PAN	Primary Account Number	Up to 10
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

### Response Message

- 8.6.25.1    A    A *successful* response to the *Get Amount 3* command shall have the format shown in table 8.96.

Table 8.96 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0010'	2
Transaction Amount	Transaction Amount	4
CURR	Currency Code and exponent	3
LEN <sub>DD</sub>	'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 8.97.

Table 8.97 – 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

## 8.7 Local PIN Commands

### 8.7.1 Load LP Keys Command – Method Number 1

#### Command Message

The *Load LP Keys* command has the format shown in table 8.98.

Table 8.98 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1	
L <sub>DATA</sub>	'0020'	2	
CLA	'B1'	1	
INS	'00'	1	
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2	
L <sub>c</sub>	'1A'	1	
ID <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1	
Method Number	'01' (Enciphered)	1	
LEN <sub>MSCD</sub>	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 <sub>e</sub>	'00'	1	

- 8.7.1.1 A DES encipherment of the Keys shall be performed using ECB mode.

#### Response Message

- 8.7.1.2 A A *successful* response to the *Load LP Keys* command shall have the format shown in table 8.99.



Table 8.99 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'000A'	2
Method Number	'01' (Enciphered)	1
LEN <sub>MSRD</sub>	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

## 8.7.2 Local PIN Validation

### Command Message

The *Local PIN Validation (Plaintext)* command has the format shown in table 8.100.

Table 8.100 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'001C' or '0023'	2
CLA	'B1'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'16' or '1D'	1
ID <sub>THREAD</sub>	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 <sub>AMOUNT</sub>	Length of amount related fields ('00' if absent)	1
Amount	Transaction Amount	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
LEN <sub>MSCD</sub>	Length of Method Specific Command Data = '0008'	2
Method Specific Command Data	Plaintext PIN Block	8
L <sub>e</sub>	'00'	1

- 8.7.2.1 A LEN<sub>AMOUNT</sub> shall either have the value '00' (if absent) or '07' (if present).

### Response Message

- 8.7.2.2 A A successful response to the *Local PIN Validation (Plaintext)* command shall have the format shown in table 8.101.

Table 8.101 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'0007'	2
Method Number	'00' (Plaintext PIN Block)	1
LEN <sub>MSRD</sub>	'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 8.102.

Table 8.102 – 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 <sub>THREAD</sub>	Thread Identifier assigned by the MAD-Handler	1
L <sub>DATA</sub>	'002E' or '0035'	2
CLA	'B1'	1
INS	'80'	1
P1, P2	ID <sub>PSAMAPP</sub> = '8111'	2
L <sub>c</sub>	'28' or '2F'	1
ID <sub>THREAD</sub>	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 <sub>AMOUNT</sub>	Length of amount related fields ('00' if absent)	1
Amount	Transaction Amount	4
CURRC	Currency Code	2
CURRE	Currency Exponent	1
LEN <sub>MSCD</sub>	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 8.103 for further details)	24
L <sub>e</sub>	'00'	1

8.7.2.3 A LEN<sub>AMOUNT</sub> shall either have the value '00' (if absent) or '07' (if present).

8.7.2.4 A The Enciphered PIN Data shall have the format shown in table 8.103.

Table 8.103 – 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

- 8.7.2.5 A DES encipherment of the data listed in table 8.103 shall be performed using CBC mode.

### Response Message

- 8.7.2.6 A A *successful* response to the *Local PIN Validation (Enciphered)* command shall have the format shown in table 8.104.

Table 8.104 – 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 <sub>THREAD</sub>	Thread Identifier of the request	1
L <sub>DATA</sub>	'000B'	2
Method Number	'01' (Enciphered PIN Block)	1
LEN <sub>MSRD</sub>	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

## 8.8 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 8.108 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 8.105 – 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

### 8.8.1 Application Specific ASW1–ASW2 Coding (Debit/Credit)

Application Status Words (ASW1–ASW2) are grouped in categories depending of which action to take. Table 8.106 gives the ranges for each category.

Table 8.106 – ASW1–ASW2 grouping

Category	ASW1–ASW2
Approved/Successful	'0000'
Approved/Successful – Action requested	'10XX' <sup>1)</sup>
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'
Reserved	'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'
<b>Legend:</b>	
1) For the range '10FB' – '10FD', the transaction is not considered successful, but fallback using magnetic stripe technology is allowed.	

8.8.1.1 A Conversion of Application Status Words to Message Codes is given in table 8.107.

8.8.1.2 A New ASW1–ASW2 not yet defined in the following tables, but inside the ranges given in table 8.107, 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 8.120 (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 6.18 (Exception Handling) and in particular subsection 6.18.2 (General Rules).

- 8.8.1.3 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.

- 8.8.1.4 B If the Message Code is ‘F3’ (Technical Failure), the Application Status Words shall be displayed after the text in the Merchant Display.

- 8.8.1.5 B Message Code ‘94’ (Suspected fraud), ‘8F’ (Pick up card) and ‘F7’ (Refer acquirer) shall only be displayed on the Merchant Display. When ‘94’, ‘8F’ or ‘F7’ is to be displayed on the Merchant Display, Message Code ‘07’ (Declined) shall be displayed on the Cardholder Display.



Table 8.107 – ASW1–ASW2 Converted to Message Codes

ASW1–ASW2 Range		Message Code	Text	
From	To		English	Danish
'0000'	'0000'	'03'	Approved	Godkendt
'0001'	'0FFF'	'F3'	Technical failure	Teknisk fejl
'1000'	'10FA'	'03'	Approved	Godkendt
'10FB'	'10FD'	'0C'/'12' <sup>1)</sup>	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	Beløb for højt
'1270'	'1274'	'94' <sup>2)</sup>	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' <sup>2)</sup>	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
'1400'	'140F'	'0C'	Not accepted	Kan ikke anvendes
'1410'	'141F'	'AF'	Invalid currency	Ugyldig valuta
'1420'	'142F'	'EE'	Insert card again	Indlæs kort igen

**Legend:**

1) Message Code '12' shall only be displayed when the requirements stated in section 5.14 are fulfilled. Message Code '0C' and '12' should preferably be shown simultaneously, alternatively alternating.

2) For Message Code '94', '8F' and 'F7', see requirement 8.8.1.5.

Table 8.107 – ASW1–ASW2 Converted to Message Codes (*Concluded*)

ASW1–ASW2 Range		Message Code	Text	
From	To		English	Danish
'1430'	'14FF'	'F3'	Technical failure	Teknisk fejl
'1500'	'15FF'	'8F' <sup>2)</sup>	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'	'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 5.14 are fulfilled. Message Code '0C' and '12' should preferably be shown simultaneously, alternatively alternating.

2) For Message Code '94', '8F' and 'F7', see requirement 8.8.1.5.

Table 8.108 – Approved/Successful

ASW1–ASW2	APACS	Meaning	Description
'0000'	0000	Successful	No further action

Table 8.109 – 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> 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
'1020'		No issuer response	–
'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
'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
'1058'	–	Mandatory data is missing 1	–
'1059'	–	Redundant data objects (command)	Redundant primitive data objects read in the command

Table 8.109 – Approved/Successful – Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'105A'	–	Thread unknown (soft)	Only applicable for the <i>Complete &amp; 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
'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	The PSAMs Certification Authority Public Key Index is not equal to VPKI <sub>IEP</sub> 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'	–	DDA hash algorithm not supported	–
'107A'	–	DDA hash result invalid	–
'107B'	–	SDA hash algorithm not supported	–
'107C'	–	SDA hash result invalid	–

Table 8.109 – Approved/Successful – Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'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
'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
'1094'	–	Header/Trailer format error	CDA specific
'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	VKPCA, 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

Table 8.109 – Approved/Successful – Action Requested (*concluded*)

ASW1-ASW2	APACS	Meaning	Description
'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	–
'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
'10FB'	–	Fallback allowed	See conditions in section 5.14
'10FC'	–	RFU (Fallback handling)	–
'10FD'	–	RFU (Fallback handling)	–
'10FF'	–	Incorrect PIN, next CVM selected	Display message code '0A' "Incorrect PIN" for 6 seconds

Table 8.110 – 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 <sub>THREAD</sub> is not correct for the command. For example, the ID <sub>THREAD</sub> 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 <sub>C</sub> error	The length field L <sub>C</sub> does not match the actual length
'1130'	–	LEN <sub>APDU</sub> 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'	–	Key is missing	–
'1137'	–	LEN <sub>MDOL</sub> error	–
'1140'	–	Data Store Handler must be opened	The terminal must resolve the problem by sending the Open Handler message to the Data Store Handler.

Table 8.110 – Error – Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'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.
'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
'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	–
'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	–



Table 8.110 – Error – Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'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)	–
'118C'	–	LEN <sub>STAT</sub> 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	–
'1192'	–	POS Entry Mode invalid for this Token	Position 1 & 2 of POS Entry Mode are not identical to the terminal that created the Token
'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'	–	Tamper Evident 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	–

Table 8.110 – Error – Action Requested (*continued*)

ASW1–ASW2	APACS	Meaning	Description
'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 <sub>CA, PSAM</sub> 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
'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	–
'11E6'	–	State address not found	–
'11E7'	–	Command address not found	–

Table 8.110 – Error – Action Requested (*concluded*)

ASW1–ASW2	APACS	Meaning	Description
'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'	–	Length of Token invalid	–

Table 8.111 – 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
'120F'	–	Voice authorization rejected	–
'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	–

Table 8.111 – Declined (*continued*)

ASW1-ASW2	APACS	Meaning	Description
'1225'	–	Service not allowed	–
'1237'	–	Track2 Equivalent Data length error	Length exceeds 37 characters
'1226'	–	CDA failed	–
'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
'1240'	1001	Expired card	–
'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
'1280'	1026	Invalid PIN block	–
'1281'	1027	PIN length error	–
'1282'	1028	PIN key synchronization error	–
'1290'	1023	Exceeds withdrawal frequency limit	–
'12A0'		Forced offline not allowed	Request for offline transaction is not accepted by the PSAM
'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	–
'12B5'	1014	No account of type requested	–
'12B6'	1015	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	–

Table 8.111 – Declined (*concluded*)

ASW1–ASW2	APACS	Meaning	Description
'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
'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	–
'1320'	–	External authentication error	External authentication sent to the card was rejected
'1321'	–	AC data error	Application Cryptogram data error (transaction related data)
'1322'	–	Wrong cryptogram	Cryptogram is not the requested

Table 8.112 – 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 8.113 – 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 8.114 – 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 <sup>1)</sup>	Cutover in progress	–
'1604'/'1020'	5407 <sup>1)</sup>	Card issuer or switch inoperative	–
'1605'	5408	Transaction destination cannot be found for routing	–
'1606'	5409	System malfunction	–
'1607'/'1020'	5410 <sup>1)</sup>	Card issuer signed off	–
'1608'/'1020'	5411 <sup>1)</sup>	Card issuer timed out	–
'1609'/'1020'	5412 <sup>1)</sup>	Card issuer unavailable	–
'160A'	5414	Not able to trace back to original transaction	–
'160B'/'1020'	5415 <sup>1)</sup>	Reconciliation cutover or checkpoint error	–
'160C'	5316	MAC incorrect	–
'160D'	5417	MAC key synchronization error	–
'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 <sup>1)</sup>	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)	*****

**Legend:** <sup>1)</sup> 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 of-line or be rejected.

Table 8.114 – Failed – Retry (*concluded*)

ASW1–ASW2	APACS	Meaning	Description
'1630'	–	Invalid data received	–
'1631'	–	MTI error	–
'1632'	–	Bit map error	Primary Message bitmap is not as expected
'1633'	–	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	–
'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
<b>Legend:</b> <sup>1)</sup> 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 be approved or rejected.			

Table 8.115 – 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
'171E'	–	Service Code; format error	–
'176D'	–	Transaction Request illegal	The Transaction Request is not in the legal range
'176E'	–	LEN <sub>TRACK2</sub> error	–
'1770'	6005	Acquirer not supported by switch	–
'1780'	6002	Invalid transaction	–
'17A0'	6013	Duplicate transmission	–
'17A1'	6022	Message number out of sequence	–
'17A2'	6050	Violation of business arrangement	–

Table 8.116 – 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 8.117 – 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</i> command shall be issued after the <i>Complete Payment</i> command
'1B86'	–	PIN not available	–
'1B87'	–	Tamper Evident 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 <sub>CA</sub> , 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 8.118 – 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	–

Table 8.119 – 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 8.120 – Debit/Credit PSAM generated ASW1–ASW2s (1)

ASW1–ASW2	Meaning	Commands	S t a r t U p	S u p p o r t e d	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	
'00xx'	<b>Successful (TAPA defined)</b>																	
'0000'	Successful		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'02xx'	<b>(TAPA defined)</b>																	
'0200'	No information given		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'0201'	Application not supported		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'0202'	Function not supported		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'0203'	PIN Pad is unresponsive													*				
'0204'	PIN Pad unable to synchronize												*					
'10xx'	<b>Approved/Successful – Action Requested</b>																	
'1000'	Configuration required		*	*	*			*				*						
'1001'	Installation required		*					*										
'1002'	Restart required		*	*	*	*	*	*				*	*		*			
'1003'	New data available		*	*	*			*				*	*	*				
'1010'	Approved (VIP)																	
'1011'	Approved, update ICC																	
'1012'	Approved (National use)																	
'1013'	Approved (National use)																	
'1014'	Approved (National use)																	
'1015'	Approved (National use)																	
'1016'	Approved (National use)																	
'1020'	No issuer response																	
'1030'	No CVM performed successfully																	
'1031'	Offline PIN validation failed																	
'1032'	PAN mismatch																	
'1033'	Requested transaction not found															*		
'1034'	Format error in host message, offline approved															*		
'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																	
'1058'	Mandatory data is missing 1																	
'1059'	Redundant data objects (command)																	
'105F'	Length of modulus does not match Issuer Certificate																	
'105A'	Thread unknown (soft)																	
'1060'	Issuer Certificate format error																	
'1061'	Issuer Certificate invalid																	
'1062'	Issuer Identification Number mismatch																	
'1063'	Card Certificate format error																	

Table 8.120 – 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	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 a t e I n	G e t D / C P r o p	S e t D / C P r o p	
'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'	DOL data out of range																	
'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'	DDA hash algorithm not supported																	
'107A'	DDA 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																	
'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																	

Table 8.120 – 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	
'1093'	Hash (Transaction Data) wrong																	
'1094'	Header/Trailer format error																	
'10B2'	Refer to card issuer																	
'10B3'	Refer to card issuer's special conditions																	
'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																	
'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 AID length																*	

Table 8.120 – 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	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 a t e	G e t D / C P r o p	S e t D / C P r o p	
'10EF'	AID not found in AID Table															*		
'10F0'	PAN not found in MSC Table															*		
'10F1'	Syntax error (input data)															*		
'10F2'	Local PIN disabled															*		
'10FB'	Fallback allowed																	
'10FF'	Incorrect PIN, next CVM selected																	
<b>'11xx' Error – Action Requested</b>																		
'1100'	Start-up PSAM command required		*	*	*	*	*	*	*	*	*	*	*	*	*			
'1101'	Restart required																	
'1110'	Outstanding transaction must be completed		*															
'1111'	Command out of sequence		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1120'	Data 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 long											*						
'112E'	Tag changed between segments											*						
'112F'	L <sub>c</sub> error		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1130'	LEN <sub>APDU</sub> error		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1131'	MAC error in command											*						
'1132'	MDOL2 data present																	
'1133'	MDOL1 data missing																	
'1134'	MDOL2 data missing																	
'1135'	Counter number out of range											*						
'1136'	Key is missing											*						
'1137'	LEN <sub>MDOL</sub> error																	
'1140'	Data Store Handler must be opened																	
'1141'	Data Store full																	
'1142'	Duplicate File IDs					*												
'1143'	Invalid File ID					*												

Table 8.120 – 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 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	
'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																	
'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																	
'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																	

Table 8.120 – 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 I n	G e t D / C P r o p	S e t D / C P r o p	
'118B'	Authentication error (MAC validation failed)																	
'118C'	LEN <sub>STAT</sub> 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																	
'1192'	POS Entry Mode invalid for this Token																	
'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'	Tamper Evident 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 8.120 – 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	
'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'	Length of Token invalid																	
'12xx' – '13xx'	<b>Declined</b>																	
'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)																	

Table 8.120 – 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 I n	G e t D / C P r o p	S e t D / C P r o p	
'120D'	Data are inconsistent with original data (National use)																	
'120E'	Transaction declined by ICC																	
'120F'	Voice authorization rejected																	
'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																	
'1280'	Invalid PIN block																	
'1281'	PIN length error																	
'1282'	PIN key synchronization error																	
'1290'	Exceeds withdrawal frequency limit																	
'12A0'	Forced offline not allowed																	
'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																	

Table 8.120 – 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	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 a t e I n	G e t D / C P r o p	S e t D / C P r o p	
'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																	
'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																	
'1320'	External authentication error																	
'1321'	AC data error																	
'1322'	Wrong cryptogram																	
'14xx'	<b>Declined – Try Again with other Parameters</b>																	
'1400'	Select other application																	
'1410'	Currency not supported																	
'1420'	Card not present																	
'15xx'	<b>Declined – Pick up</b>																	
'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'	<b>Failed – Retry</b>																	
'1600'	Condition of use not satisfied																	
'1601'	Re-enter transaction															*		
'1602'	Format error															*		

Table 8.120 – 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 I n	G e t D / C P r o p	S e t D / C P r o p
'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														*		
'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'	Illegal 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															*	
'1650'	All entries in use – New thread cannot be started																
'1651'	Fatal error		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1652'	Fatal command error		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

Table 8.120 – 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	
'17xx'	<b>Failed – No Retry</b>																	
'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																	
'171E'	Service Code; format error																	
'1760'	Data not found																	
'1761'	Data Store error – No information given																	
'176D'	Transaction request illegal																	
'176E'	LEN <sub>TRACK2</sub> error																	
'1770'	Acquirer not supported by switch														*			
'1780'	Invalid transaction														*			
'17A0'	Duplicate transaction														*			
'17A1'	Message number out of sequence														*			
'17A2'	Violation of business arrangement														*			
'1Axx'	<b>RC Related (Card Handler)</b>																	
'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																	
'1AF5'	Handler busy																	
'1AF6'	Insufficient resources																	
'1AF7'	Handler must be opened																	
'1AFB'	Unsupported operation																	
'1Bxx'	<b>RC Related (User Interface Handler)</b>																	
'1B34'	Unknown Message Code														*			
'1B35'	Code Table not supported														*			
'1B80'	No KCV available, KSES not present														*			

Table 8.120 – 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 I n	G e t D / C P r o p	S e t D / C P r o p
'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'	Tamper Evident 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 <sub>CA</sub> , 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		*	*	*	*	*	*	*	*	*	*	*	*	*		
'1BF8'	Unsupported operation		*	*	*	*	*	*	*	*	*	*	*	*	*		
'1Cxx'	<b>RC Related (Merchant Application Handler)</b>																
'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		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1CF8'	Unsupported operation		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1Dxx'	<b>RC Related (Data Store Handler)</b>																
'1D51'	Invalid File ID																
'1D52'	Record too large																
'1D53'	Search key too large																
'1D55'	File could not be accessed																
'1D57'	File read error																

Table 8.120 – Debit/Credit PSAM generated ASW1–ASW2s (1) (concluded)

ASW1–ASW2	Meaning	Commands	S	S	M	F	C	E	I	A	D	P	S	C	V	G	S
			t	u	s	i	h	n	d	d	s	s	r	a	e	e	e
			Start	Up	IDs	Table	Charac	tere	ng	all	um	ivate	date	ize	in	prop	prop
	'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	*	*	*	*	*	*	*	*	*	*	*	*			
<b>'61xx' – '6Fxx' Card errors conveyed transparently</b>																	
	'61L <sub>a</sub> '	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															
<b>'91xx' – '9Fxx' Card errors conveyed transparently</b>																	

Table 8.121 – 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		
<b>'00xx'</b>		<b>Successful (TAPA defined)</b>																	
	'0000'	Successful	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
<b>'02xx'</b>		<b>(TAPA defined)</b>																	
	'0200'	No information given	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	'0201'	Application not supported	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	'0202'	Function not supported	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	'0203'	PIN Pad is unresponsive	*	*															
	'0204'	PIN Pad unable to synchronize	*	*															
<b>'10xx'</b>		<b>Approved/Successful – Action Requested</b>																	
	'1000'	Configuration required																	
	'1001'	Installation required																	
	'1002'	Restart required																	
	'1003'	New data available																	
	'1010'	Approved (VIP)								*	*	*	*						
	'1011'	Approved, update ICC								*	*	*	*						
	'1012'	Approved (National use)								*	*	*	*						
	'1013'	Approved (National use)								*	*	*	*						
	'1014'	Approved (National use)								*	*	*	*						
	'1015'	Approved (National use)								*	*	*	*						
	'1016'	Approved (National use)								*	*	*	*						
	'1020'	No issuer response								*									
	'1030'	No CVM performed successfully	*																
	'1031'	Offline PIN validation failed	*																
	'1032'	PAN mismatch	*																
	'1033'	Requested transaction not found																	
	'1034'	Format error in host message, offline approved								*									
	'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														*	*	*	*
	'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	*																



Table 8.121 – 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
'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'	DDA hash algorithm not supported	*															
'107A'	DDA 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									*							
'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					*											
'10B2'	Refer to card issuer	*															
'10B3'	Refer to card issuer's special conditions	*															
'10CB'	PIN Pad PK record not found	*															

Table 8.121 – 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
'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	*															
'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 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	*															
'10FB'	Fallback allowed	*														*	
'10FF'	Incorrect PIN, next CVM selected	*															
'11xx'	<b>Error – Action Requested</b>																
'1100'	Start-up PSAM command required	*	*	*	*												

Table 8.121 – 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	
'1101'	Restart required																	
'1110'	Outstanding transaction must be completed	*	*	*	*													
'1111'	Command out of sequence	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1120'	Data 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 long																	
'112E'	Tag changed between segments																	
'112F'	L <sub>c</sub> error	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1130'	LEN <sub>APDU</sub> error	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1131'	MAC error in command																	
'1132'	MDOL2 data present																	
'1133'	MDOL1 data missing					*	*											
'1134'	MDOL2 data missing									*	*							
'1135'	Counter number out of range																	
'1136'	Key is missing																	
'1137'	LEN <sub>MDOL</sub> error					*	*			*	*							
'1140'	Data Store Handler must be opened															*	*	*
'1141'	Data Store full														*	*	*	*
'1142'	Duplicate File IDs																	
'1143'	Invalid File ID														*	*	*	*
'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																	
'1160'	Tag format error	*																

Table 8.121 – Debit/Credit PSAM generated ASW1–ASW2s (2) (continued)

ASW1–ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	S C	K Y	T O K	E M V	S C	K Y	T O K	E M V	S C	K Y	T O K	E M V	S C	K Y	T O K
'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	*															
'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 <sub>STAT</sub> 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				*												
'1192'	POS Entry Mode invalid for this Token				*												
'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'	Tamper Evident Device not in PIN Entry State																

Table 8.121 – 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
'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																
'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				*												

Table 8.121 – 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	
'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'	Length of Token invalid									*								
<b>'12xx' – '13xx' Declined</b>																		
'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					*	*	*										
'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)										*	*	*	*				
'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	*	*	*														

Table 8.121 – 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
'1262'	Amount exceeds offline ceiling									*							
'1270'	Suspected fraud									*	*	*	*				
'1271'	Suspected counterfeit card									*	*	*	*				
'1275'	Amount not confirmed/accepted	*	*	*	*												
'1276'	Transaction interrupted									*	*	*	*	*	*	*	*
'1280'	Invalid PIN block	*	*							*	*	*	*				
'1281'	PIN length error	*	*							*	*	*	*				
'1282'	PIN key synchronization error									*	*	*	*				
'1290'	Exceeds withdrawal frequency limit									*	*	*	*				
'12A0'	Forced offline not allowed					*	*	*	*	*	*	*	*				
'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	*															
'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									*	*	*	*				
'1320'	External authentication error																
'1321'	AC data error																
'1322'	Wrong cryptogram																
'14xx'	<b>Declined – Try Again with other Parameters</b>																
'1400'	Select other application	*														*	
'1410'	Currency not supported	*	*	*	*												
'1420'	Card not present																

Table 8.121 – 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
<b>'15xx' Declined – Pick up</b>																	
'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					*	*	*									
<b>'16xx' Failed – Retry</b>																	
'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 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									*	*	*	*				



Table 8.121 – 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
'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		*														
'1650'	All entries in use – New thread cannot be started	*	*	*	*												
'1651'	Fatal error	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'1652'	Fatal command error	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
'17xx'	<b>Failed – No Retry</b>																
'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													*	*	*	*
'171E'	Service Code; format error																
'1760'	Data not found	*				*				*							
'1761'	Data Store error – No information given													*	*	*	*
'176D'	Transaction request illegal	*	*	*	*												
'176E'	LENT <sub>TRACK2</sub> error		*														
'1770'	Acquirer not supported by switch									*	*	*	*				
'1780'	Invalid transaction									*	*	*	*				
'17A0'	Duplicate transaction									*	*	*	*				
'17A1'	Message number out of sequence									*	*	*	*				
'17A2'	Violation of business arrangement									*	*	*	*				
'1Axx'	<b>RC Related (Card Handler)</b>																
'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	*															

Table 8.121 – Debit/Credit PSAM generated ASW1-ASW2s (2) (continued)

ASW1-ASW2	Meaning	Initiate				Payment				Validate				Complete			
		E M V	S C	K Y	T O K	E M V	S C	K Y	T O K	E M V	S C	K Y	T O K	E M V	S C	K Y	T O K
'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	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
<b>'1Bxx' RC Related (User Interface Handler)</b>																	
'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'	Tamper Evident 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. VKPCA, 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	*	*	*	*	*	*	*	*					*	*	*	*
<b>'1Cxx' RC Related (Merchant Application Handler)</b>																	
'1C40'	Invalid Currency	*	*	*													
'1C41'	Invalid Currency Exponent	*	*	*													
'1CF2'	Time-out	*	*	*	*	*	*	*	*					*	*	*	*
'1CF3'	Handler error	*	*	*	*	*	*	*	*					*	*	*	*
'1CF4'	Handler must be initialized	*	*	*	*	*	*	*	*					*	*	*	*
'1CF5'	Handler busy	*	*	*	*	*	*	*	*					*	*	*	*

Table 8.121 – Debit/Credit PSAM generated ASW1–ASW2s (2) (concluded)

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
	'1CF6'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1CF7'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1CFB'	*	*	*	*	*	*	*	*	*				*	*	*	*
'1Dxx'	<b>RC Related (Data Store Handler)</b>																
	'1D51'													*	*	*	*
	'1D52'													*	*	*	*
	'1D53'													*	*	*	*
	'1D55'													*	*	*	*
	'1D57'													*	*	*	*
	'1D58'													*	*	*	*
	'1D59'													*	*	*	*
	'1DF2'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1DF3'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1DF4'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1DF5'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1DF6'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1DF7'	*	*	*	*	*	*	*	*	*				*	*	*	*
	'1DFB'	*	*	*	*	*	*	*	*	*				*	*	*	*
'61xx' – '6Fxx'	<b>Card errors conveyed transparently</b>																
	'61L <sub>a</sub> '	*				*											
	'6300'	*								*							
	'63Cx'	*															
	'6983'	*															
	'6984'	*															
	'6985'	*				*				*							
	'6A81'	*															
	'6A83'	*															
	'6A88'	*															
'91xx' – '9Fxx'	<b>Card errors conveyed transparently</b>																
		*				*				*							

## 8.8.2 ASW1–ASW2 Applicable for Local PIN

Table 8.122 – Approved/Successful

ASW1–ASW2	APACS	Meaning	Description
'0000'	–	Successful	No further action.

Table 8.123 – Approved/Successful – Action Requested

ASW1–ASW2	APACS	Meaning	Description
'10F2'	–	Local PIN disabled	Get Debit/Credit Properties

Table 8.124 – 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 <sub>AMOUNT</sub> has illegal value	Related to the <i>Local PIN Validation</i> command
'1F09'	–	LEN <sub>MSCD</sub> has illegal value (Method Number '00')	Related to the <i>Local PIN Validation</i> command
'1F0A'	–	LEN <sub>MSCD</sub> 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 <sub>c</sub> 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 8.124 – Error – Action Requested (*concluded*)

ASW1–ASW2	APACS	Meaning	Description
'1F21'	–	Load LEN <sub>MSCD</sub> 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 8.125 – 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 8.8.1.

This page is intentionally left blank

# 9. Data Elements

## 9.1 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).

### 9.1.1 Coding of Data Elements

- 9.1.1.1      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.
- 9.1.1.2      A      When a field of more than one byte has to be transmitted, the *most* significant byte shall be sent first.

### 9.1.2 Data Elements Defined in EMV and TAPA

Data elements not listed in this chapter can be found in either ref. 36: “EMV, version 4.1”, ref. 40: “TAPA, Application Architecture Specification” or in ref. 42: “TAPA CEP Application Volume 1”.

## 9.2 Data Elements for the Debit/Credit Application

### 9.2.1 Account Type

*Reference:* Ref. 36: “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 9.1.

*Remarks:* Tag ‘5F57’ is dedicated to this data element. Account Type is applicable for Service Pack 2 and onward.

Table 9.1 – Account Type

Value	Account Type
‘00’	Default – unspecified
‘10’	Savings
‘20’	Cheque/debit
‘30’	Credit
All other values RFU	

### 9.2.2 Action Code

*Reference:* Ref. 38: “APACS Standard 60” and ref. 12: “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 attachment F, section F.9.9.

*Remarks:* The Action Code is transmitted in field 39 in APACS 60 messages.

### 9.2.3 Addendum Record

*Purpose:* To hold additional information.

*Format:* LEN<sub>ADD</sub> bytes.

*Contents:* Any.

*Remarks:* See section F.9.20 for more details.



### 9.2.4 AID (Application Identifier)

*Reference:* Ref. 9: “ISO/IEC 7816–5” and ref. 36: “EMV, version 4.1” (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.

### 9.2.5 ALG<sub>VL</sub>P

*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.

### 9.2.6 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.

### 9.2.7 Amount, Other

*Purpose:* To hold a cashback amount.

*Format:* b4 (4 bytes).

*Contents:* Amount, Other is coded identically to Amount (see section 9.2.6).

### 9.2.8 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)

### 9.2.9 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

### 9.2.10 Application Label

*Reference:* Ref. 9: “ISO/IEC 7816-5” and ref. 36: “EMV, version 4.1” (tag=‘50’)

*Purpose:* Mnemonic associated with the AID.

*Format:* an1..16. Characters coded according to ref. 15: “ISO/IEC 8859-15”.

*Contents:* Alpha and numeric characters.

### 9.2.11 Approval Code

*Purpose:* Response identification assigned by the authorizing institution (or its agent). This is commonly referred to as the authorisation 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 binary value ‘00 00 00 00 00 00’ is used as an indication of “not available”.

### 9.2.12 ASI (Application Selection Indicator)

*Reference:* Ref. 36: “EMV, version 4.1”.

*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.

### 9.2.13 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.

### 9.2.14 Card Data

*Purpose:* To hold card data in a Key Entered transaction.

*Format:* Variable length.

*Contents:* PAN || Expiry Date || CV–2

### 9.2.15 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'..'FF'	RFU

### 9.2.16 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. 15: "ISO/IEC 8859–15".

*Remarks:* Trailing blanks are used for padding.

### 9.2.17 Card Sequence Number

*Purpose:* Identifies and differentiates cards with the same PAN. Used in the APACS message.

*Format:* n3 (2 bytes).

*Contents:* BCD coded.

*Remarks:* PAN Sequence Number is a similar data element used in EMV context.

### 9.2.18 Card Service Info

*Purpose:* To indicate specific card information, which may be relevant for the terminal. This information are maintained by the PSAM.

*Format:* b1 (1 byte).

*Contents:* See table 9.2.

Table 9.2 – Coding of Card Service Info

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	x	x	Reserved for PSAM usage:
–	–	–	–	–	x	–	–	<u>Service Code:</u>
–	–	–	–	–	0	–	–	– Service Code <i>not</i> accessible
–	–	–	–	–	1	–	–	– Service Code accessible
x	x	x	x	x	–	–	–	RFU

### 9.2.19 CNT<sub>X</sub> (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<sub>ENTRIES</sub>, CNT<sub>MSC</sub>, and CNT<sub>H1H2</sub>.

### 9.2.20 CURRC (Currency Code)

*Reference:* Ref. 1: “ISO 4217” and ref. 15: “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. 15: “ISO/IEC 8859-15”.

### 9.2.21 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 4217:1995”.

*Contents:* 1 digit.

### 9.2.22 CV-2 (Card Verification, method 2)

*Purpose:* To give a higher degree of security when performing Key Entered transactions. CV-2 (called CVV-2 and CVC-2 by Visa and MasterCard) is printed in the signature panel of a card but is not included in the magnetic stripe.

*Format:* n3 (2 bytes).

*Contents:* BCD coded with trailing ‘F’ as padding. If empty filled with ‘F’.

### 9.2.23 CVM Status

*Purpose:* To indicate which type(s) of CVM that is required to perform the transaction.

*Format:* See table 9.3.

Table 9.3 – 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	x	x	–	–	–	–	–	RFU

*Remarks:* The unused bits (b8 – b6) shall be set to zero.

### 9.2.24 Data Requested

*Purpose:* To indicate which data is requested.

*Format:* b1 (1 byte).

*Contents:* ‘00’                      Token related data  
‘01’                      Key Entered Data (PAN || Expiry Date || CV–2)  
‘02’ – ‘FF’                  Reserved for Future Use

*Contents:* See table 9.4.

Table 9.4 – Coding of Data Requested

Value	Meaning
‘00’	Token related data
‘01’	Key entered data (PAN    Expiry Date    CV–2)
‘02’..‘FF’	RFU

### 9.2.25 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 only for transactions with financial impact (Purchase, Refund and Capture).  
The value is set utilizing the *Set Debit/Credit Properties* command with identifier ‘8002’.  
Default value is 10 minutes.

### 9.2.26 EMV Checksum

*Purpose:* To uniquely identify the actual terminal implementation.

*Format:* b8 (8 bytes).

*Contents:* A checksum calculated on the Terminal 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).

### 9.2.27 Expiry Date

*Reference:* Ref. 36: “EMV, version 4.1” (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 YYMM.

### 9.2.28 FILEID<sub>ADMIN</sub>

*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.

### 9.2.29 FILEID<sub>PRIORITY,n</sub>

*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.

### 9.2.30 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.

### 9.2.31 Host Request

*Purpose:* To hold a host request message.

*Format:*  $LEN_{HREQ}$  bytes.

*Contents:* Any.

*Remarks:* Host Request is supplied by the PBS PSAM.

### 9.2.32 Host Response

*Purpose:* To hold host response data.

*Format:*  $LEN_{HR}$  bytes.

*Contents:* Any.

### 9.2.33 $ID_{PSAM}$ (Identifier for a PSAM)

*Purpose:* To uniquely identify each PSAM

*Format:* b4 (4 bytes).

*Contents:* At the discretion of the PSAM Creator

### 9.2.34 $ID_{PSAMAPP}$ (TAPA PSAM Application Identifier)

*Purpose:* To identify a particular PSAM application.

*Format:* b2 (2 bytes).

*Contents:* '8111' indicates PBS Debit/Credit application according to this specification.

### 9.2.35 $ID_{PSAMCREATOR}$

*Purpose:* Identify the creator of the PSAM. Ref. 40: "TAPA, Application Architecture Specification".

*Format:* b4 (4 bytes).

*Remarks:* Assigned by the owner of the  $RID_{PSAM}$ .

### 9.2.36 $ID_{PSAMCREATOR}$

*Purpose:* To uniquely identify each PSAM Creator

*Format:* b4 (4 bytes).

*Remarks:* Assigned by the owner of the  $RID_{PSAM}$ .

### 9.2.37 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 9.5.

Table 9.5 – 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>State information:</u>
–	–	–	–	–	–	0	–	– Status is <i>not</i> requested
–	–	–	–	–	–	1	–	– Status is requested
–	–	–	–	–	x	–	–	<u>Original 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.

### 9.2.38 Issuer DD (Issuer Discretionary Data in FCI)

**Reference:** Ref. 36: “EMV, version 4.1” (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.

### 9.2.39 Issuer Envelope Data

**Purpose:** To hold issuer related data conveyed transparently to the issuer e.g. loyalty related data.

**Format:** b..60 (60 bytes)/b..150 (150 bytes).

**Contents:** At the discretion of the Issuer.

**Remarks:** When the Issuer Envelope Data is conveyed during an EMV transaction, the number of bytes are limited to 60 bytes. The maximum size for MSC is 150 bytes.

### 9.2.40 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.

### 9.2.41 LEN<sub>x</sub> (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’ indicates that the corresponding data element/structure is absent.

*Remarks:* Examples of use are: LEN<sub>ADD</sub>, LEN<sub>AID</sub>, LEN<sub>AMOUNTS</sub>, LEN<sub>AT</sub>, LEN<sub>CARDDATA</sub>, LEN<sub>DATA</sub>, LEN<sub>HR</sub>, LEN<sub>HREQ</sub>, LEN<sub>IDD</sub>, LEN<sub>MDOL1</sub>, LEN<sub>MDOL2</sub>, LEN<sub>PAN</sub>, LEN<sub>PDOL</sub>, LEN<sub>STAT</sub>, LEN<sub>TOKEN</sub>, LEN<sub>TRACK2</sub>, LEN<sub>UPD</sub>.

### 9.2.42 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.

### 9.2.43 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’.

### 9.2.44 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 F.95.

### 9.2.45 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 re-

side in the PSAM. Candidates for the MDOL are the data elements which origin in the terminal.

#### 9.2.46 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.

#### 9.2.47 ME<sub>ADDRESS</sub> (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. 15: “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.

#### 9.2.48 ME<sub>BRN</sub> (Business Registration Number)

*Purpose:* To indicate the Business Registration Number for the merchant.

*Format:* anps12 (12 bytes).

*Contents:* Characters coded according to ref. 15: “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.

#### 9.2.49 ME<sub>CITY</sub> (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. 15: “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.

#### 9.2.50 ME<sub>NAME</sub> (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. 15: “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.

#### 9.2.51 ME<sub>NUMBER</sub> (Merchant Number)

*Purpose:* To indicate the ID of the merchant where the terminal is located.  
The Merchant Number is unique within a given PBS defined debit/credit application.

*Format:* n10 (5 bytes).

*Contents:* BCD coded.

*Remarks:* The Merchant Number is printed on the cardholder receipt.

### 9.2.52 ME<sub>PHONE</sub> (Merchant Phone No.)

*Purpose:* To indicate the phone number of the merchant where the terminal is located (or a central helpdesk).

*Format:* ansp24 (24 bytes).

*Contents:* Characters coded according to ref. 15: “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.

### 9.2.53 ME<sub>ZIP</sub> (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. 15: “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.

### 9.2.54 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 9.6.

Table 9.6 – Coding of Merchant Initiative

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	–	–	–	–	–	–	–	<u>Forced CVM:</u>
0	–	–	–	–	–	–	–	– CVM not forced, ignore b2–b1
1	–	–	–	–	–	–	–	– CVM forced, see b2–b1
–	–	–	–	–	–	–	x	<u>PIN:</u>
–	–	–	–	–	–	–	0	– PIN <i>not</i> to be verified
–	–	–	–	–	–	–	1	– PIN to be verified
–	–	–	–	–	–	x	–	<u>Signature:</u>
–	–	–	–	–	–	0	–	– Signature <i>not</i> to be requested
–	–	–	–	–	–	1	–	– Signature to be requested
–	x	–	–	–	–	–	–	<u>Forced Online/Offline:</u>
–	0	–	–	–	–	–	–	– Not forced Online/Offline, ignore b6–b5
–	1	–	–	–	–	–	–	– Forced Online/Offline, see b6–b5
–	–	–	x	–	–	–	–	<u>Online:</u>
–	–	–	0	–	–	–	–	– Online <i>not</i> to be requested
–	–	–	1	–	–	–	–	– Online to be requested
–	–	x	–	–	–	–	–	<u>Offline:</u>
–	–	0	–	–	–	–	–	– Offline <i>not</i> to be requested
–	–	1	–	–	–	–	–	– Offline to be requested
–	–	–	–	–	x	–	–	<u>Override Amount Limits:</u>
–	–	–	–	–	0	–	–	– Amount limits effective
–	–	–	–	–	(1)	–	–	– Not allowed
–	–	–	–	x	–	–	–	<u>Addendum Record:</u>
–	–	–	–	0	–	–	–	– Addendum Record(s) <i>not</i> to be attached
–	–	–	–	1	–	–	–	– Addendum Record(s) to be attached

**Remarks:** Conflicting values (e.g. PIN & Signature forced) will result in rejection.  
Forcing CVM (b8 = 1) without setting any of the corresponding bits for a specific CVM (b2 or b1) will result in rejection, i.e. No CVM cannot be forced.  
Forcing Online/Offline (b7 = 1) without setting any of the corresponding bits (b6 or b5) will result in rejection.

### 9.2.55 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.

### 9.2.56 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)

### 9.2.57 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 ‘F’s as padding (more occurrences are accepted).

### 9.2.58 PAN Sequence Number

*Purpose:* Identifies and differentiates cards with the same PAN.

*Format:* n2 (1 byte).

*Contents:* BCD coded.

*Remarks:* Card Sequence Number is used in APACS messages.

### 9.2.59 PAN<sub>FROM</sub>

*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<sub>FROM</sub> value is included in the prefix range.

### 9.2.60 PAN<sub>TO</sub>

*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<sub>TO</sub> value is included in the range.

### 9.2.61 PIN Data

*Purpose:* To hold PIN related data.

*Format:* LPKM<sub>pp</sub> bytes.

*Remarks:* The data is encrypted under the PIN Pads public key.

### 9.2.62 POS Capability Code

*Reference:* Ref. 38: “APACS Standard 60”.

*Purpose:* To indicate the capabilities of the terminal in which the transaction was created.

*Format:* an6.

*Contents:* See attachment F, section F.9.4.

*Remarks:* The POS Capability Code is transmitted in field 21 in APACS 60 messages.

### 9.2.63 POS Entry Mode

*Reference:* Ref. 38: “APACS Standard 60”.

*Purpose:* To indicate the circumstances under which the transaction was created.

*Format:* n6 (3 bytes).

*Contents:* See attachment F, section F.9.5.

*Remarks:* The POS Entry Mode is transmitted in field 22 in APACS 60 messages.

### 9.2.64 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.

### 9.2.65 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.

### 9.2.66 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.

### 9.2.67 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 shall increase.

### 9.2.68 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 shall increase. PSAM Version is indicated in the Historical Characters of the Answer-to-Reset.

### 9.2.69 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.

### 9.2.70 RID<sub>PSAM</sub>

*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<sub>PSAMCREATOR</sub>), assigned as specified in ref. 9: “ISO/IEC 7816–5”.

### 9.2.71 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.

### 9.2.72 Service Packs Supported

*Purpose:* Indicating the Service Packs supported by the PSAM.

*Format:* b1 (1 byte).

*Contents:* See table 9.7.

*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 9.7 – 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

### 9.2.73 Signature Verification

*Purpose:* To indicate whether signature verification by the merchant is required or not.

*Format:* b1 (1 byte).

*Contents:* See table 9.8.

*Remarks:* Part of the response to *Exchange Debit/Credit Static information* command.

Table 9.8 – Coding of Signature Verification

Value	Meaning
'00'	Signature verification is not required
'FF'	Signature verification is required
'01'..'FE'	RFU

### 9.2.74 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.



### 9.2.75 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.

### 9.2.76 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 Attachment F, section F.9.11.

*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.

### 9.2.77 Stop List Status

*Purpose:* To indicate the result of a search in the Stop List.

*Format:* b1 (1 byte).

*Contents:* See table 9.9.

Table 9.9 – 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

### 9.2.78 Terminal Approval No.

*Purpose:* To uniquely identify a certified terminal.

*Format:* b2 (2 bytes).

*Contents:* A unique terminal identifier assigned by PBS, in the format shown in table 9.10 and 9.11.

Table 9.10 – 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 PBS</u>

Table 9.11 – 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 (CAT)
x	x	x	x	–	–	–	–	– RFU
–	–	–	–	x	x	x	x	<u>Serial Number</u>

### 9.2.79 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.

### 9.2.80 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’.

### 9.2.81 Terminal Manufacturer ID

*Purpose:* To uniquely identify a Terminal Manufacturer.

*Format:* ans3.

*Contents:* At the discretion of PBS.

*Remarks:* Part of the MAD–Handler ID. See table F.95.

### 9.2.82 Terminal Serial Number

*Purpose:* To uniquely identify a terminal under a specific Terminal Manufacturer.

*Format:* ans5.

*Contents:* At the discretion of PBS.

*Remarks:* Part of the MAD–Handler ID. See table F.95.

### 9.2.83 Terminal Settings

*Purpose:* Defines the requested behavior of the terminal/PSAM during a transaction.

*Format:* b1 (1 byte).

*Contents:* See table 9.12.

*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 9.12 – Terminal Settings

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
–	–	–	–	–	–	–	1	– Multi-entry requested
x	x	x	x	x	x	x		– RFU

### 9.2.84 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 6.5, “Tokens”.

### 9.2.85 TRACK2 DATA

*Purpose:* To hold track 2 data read on an MSC.

*Format:* Variable, up to 19 bytes long.

*Contents:* Card data according to POS Entry Mode

*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 and end sentinels and the LRC character.

### 9.2.86 Transaction Category Code

*Purpose:* Used in Card Risk Management by MasterCard applications.

*Format:* b1 (1 byte).

*Contents:* A character coded according to ref. 15: “ISO/IEC 8859–15”.

*Remarks:* This is a MasterCard specific data element. Ref. 44: “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.

### 9.2.87 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.

### 9.2.88 Transaction Request (TR)

*Purpose:* To indicate to the PSAM which transaction type should be initiated.

*Format:* b1 (1 byte).

*Contents:* See table 9.13.

Table 9.13 – Coding of Transaction Request

Value	Meaning
'00'	Purchase
'01'	Refund
'02'	Original Authorization
'03'	Supplementary Authorization
'04'	Capture
'05'	Reversal (Authorization)
'06'..'FF'	RFU

### 9.2.89 Transaction State Information

*Purpose:* To indicate the transaction progress to the Merchant Application.

*Format:* b1 (1 byte).

*Contents:* See table 9.14.

Table 9.14 – 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

### 9.2.90 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 9.15.

Table 9.15 – Coding of Transaction Status

Value	Meaning
'00'..'7F'	<u>Successful:</u>
'00'	Successful
'01'	Signature accepted
'02'..'7F'	RFU
'80'..'FF'	<u>Declined:</u>
'80'	Transaction aborted
'81'	Signature rejected
'82'	Goods or service not delivered
'83'..'FF'	RFU

### 9.2.91 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 9.2.6: “Amount”. The value represents the lowest denominator for the corresponding Currency Code, e.g. for DKK, amounts are represented in 1/100 DKK units.

### 9.2.92 Transaction Type (TT)

*Purpose:* To indicate the type of transaction according to ref. 36: “EMV, version 4.1”.

*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

### 9.2.93 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<sub>PSAMAPP</sub>.

*Format:* an20.

*Contents:* ID<sub>PSAMAPP</sub> = '8111': “PBS Debet/Kredit”.

*Remarks:* If more than one application is supported, the display may alter between the texts.

### 9.2.94 Update Data

*Purpose:* To hold PSAM update data.

*Format:* LEN<sub>UPD</sub> bytes. The format is Tag specific.

*Contents:* The content of Update Data is identified by Tag.

### 9.2.95 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

## 9.3 Data Elements specific for the Local PIN Application

### 9.3.1 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.

### 9.3.2 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.

### 9.3.3 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.

### 9.3.4 LP-KEK-Version

*Purpose:* To indicate the version of the Key Exchange Key (KEK).

*Format:* b1 (1 byte).

*Contents:* ‘00’ – ‘FF’.

### 9.3.5 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.

### 9.3.6 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.

### 9.3.7 LP-Key-Version

*Purpose:* To indicate the version of the LP-Key.

*Format:* b1 (1 byte).

*Contents:* ‘00’ – ‘FF’.

### 9.3.8 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’.

### 9.3.9 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.

### 9.3.10 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’

### 9.3.11 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.



### 9.3.12 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.

### 9.3.13 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.

### 9.3.14 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  $\neq$  '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 is between 1 to 14, the transaction counter will be incremented. Initial value of the PSAM transaction counter is zero.

This page is intentionally left blank

# 10. Design Requirements

## 10.1 General Considerations

### 10.1.1 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 misoperations do not occur. These precautions should cover:

- Climatic environments:  
temperature and humidity
- Mechanical environments:  
vibrations, impacts, shakes, collapses
- Electrical environments:  
safety, high voltage interference, immunity, fluctuations, disturbances
- Auditory environment:  
noise

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.

10.1.1.1 A The terminal shall be designed for unattended intermittent or continuous operation.

10.1.1.2 A The Terminal Supplier has the responsibility to ensure that the terminal complies with regulations specified by the authorities for the environment in which the terminal is to be installed.

**NOTE:** The Terminal Supplier should also consult relevant interest groups or organizations e.g. Danish Centre for Accessibility (Dansk Center for Tilgængelighed) and Danish Commerce & Services (Dansk Handel & Service).

10.1.1.3 A The Terminal Supplier shall classify the environment for which the terminal is suitable to operate.

## 10.1.2 Requirements from Third Parties

The EC act on product liability may apply to the terminal.

The authorities may require, that the terminal complies with the regulations for equipment connected to the power installations, e.g. ref. 32: “EN 60 950”.

The use of various types of components for the manufacture of a terminal and the manufacturing process itself may be regulated by environmental legislation.

The authorities may require, that the terminal complies with the EMC requirements in the EC EMC Directive. The Generic (and Product) EMC Standards covering both emission and immunity are e.g.:

- EN 50 081: Generic Emission Standard
- EN 50 082: Generic Immunity Standard

See ref. 29: “EN 50”.

- |          |   |  |
|----------|---|--|
| 10.1.2.1 | A | If the terminal can be connected to the public switched telephone network, it shall comply with ref. 50: “Telestyrelsen’s Publication 11/89 (Circular no. 27)” for connection to the public switched telephone network and ref. 28: “EN 41 003”. |
|----------|---|--|

## 10.1.3 Documentation

- |          |   |  |
|----------|---|--|
| 10.1.3.1 | B | The terminal shall be supplied with an installation guide.   |
| 10.1.3.2 | B | The installation guide shall be in English and Danish.   |
| 10.1.3.3 | 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. The manual shall also contain relevant technical information, including guidelines for PSAM replacement.  |
| 10.1.3.4 | C | The user manual may be in English and Danish.  |
| 10.1.3.5 | B | The mechanical, electrical and software design of the terminal shall be fully documented, in writing.  |
| 10.1.3.6 | B | The documentation shall include drawings of the placement of: <ul style="list-style-type: none"> <li>• the Cardholder Display,</li> <li>• the MSCR and ICCR,</li> <li>• the PIN Pad,</li> <li>• the shielding around the PIN Pad,</li> <li>• the command keys and</li> <li>• the Cardholder Keyboard,</li> </ul> the drawings shall also show the size and layout of the characters in the Cardholder Display. |
| 10.1.3.7 | B | The documentation of the electrical design shall also include:   |

- block diagram(s) and
  - a detailed description of the interfaces.
- 10.1.3.8 B The documentation of the software design shall:
- include drawing(s) and explanation of the logical structure of the software and
  - be delivered to the test operator for inspection.
- 10.1.3.9 B The documentation shall be in English.
- 10.1.3.10 C The documentation may also be in Danish.

#### 10.1.4 Marking

##### Terminal and Terminal Supplier Information

- 10.1.4.1 A Each terminal shall be marked with the name of the Terminal Supplier.
- 10.1.4.2 A Each terminal shall be marked with a type number.
- 10.1.4.3 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 H.2.2.5.

##### User Guidance

- 10.1.4.4 A User guidance shall be in Danish. 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.
- 10.1.4.5 B User guidance shall also be available in English.
- User guidance in other languages are allowed if Danish and English are available.
- 10.1.4.6 C User guidance in pictograms, drawings or pictures may be implemented. See figure 10.1 for examples.
- 10.1.4.7 C The character type of text is recommended to be Helvetica or Modern.
- 10.1.4.8 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.
- 10.1.4.9 A Terminals with a motorized MSCR shall be equipped with a pictogram showing the cardholder how to insert the MSC into the MSCR. See figure 10.1 for examples of pictograms.

- 10.1.4.10 A Terminals with an ICCR shall be equipped with a pictogram showing the cardholder how to insert the ICC into the ICCR. See figure 10.1 for examples of pictograms.

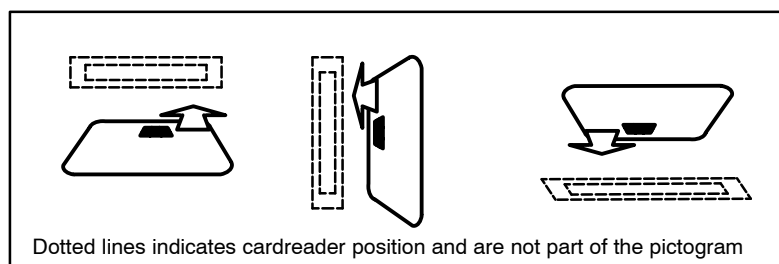


Figure 10.1 – Pictograms (Examples)

### PIN Pad

- 10.1.4.11 A The PIN Pad shall be clearly marked with the PIN Pad ID loaded into the PIN Pad.
- 10.1.4.12 C 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.

## 10.1.5 Servicing the Terminal

- 10.1.5.1 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.

## 10.2 Mechanical Design

### 10.2.1 General Requirements

- 10.2.1.1 A The terminal design of the Tamper Evident Device shall be in accordance with the requirements defined by the Payment Card Industry (PCI), see ref. 25: “POS PIN Entry Device Security Requirements Manual”.

If the ICCR or display are not part of the Tamper Evident Device, it will introduce limitations in Cardholder verification Methods supported and thus reduce the cards accepted. Furthermore, limitations concerning key entry may be introduced.

- 10.2.1.2 A Mechanical rigidity of the terminal shall be in accordance with the type of equipment and the environment in which it is installed.

- 10.2.1.3 A The terminal shall be able to withstand worst case of mechanical stress like vibrations, impacts and free fall as expected according to the environment.
- 10.2.1.4 A The PIN Pad, ICCR and Cardholder Display shall all be housed in the same tamper evident housing.
- 10.2.1.5 B For sanitary reasons the terminal shall be easy to clean as it is used by many people.
- 10.2.1.6 A Any activation of a hardware function or change in the terminal status shall cause an immediate reaction or response in the user interface.
- 10.2.1.7 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:  $\pm 3$  seconds per day and
  - battery back-up for minimum 30 days.

### Noise

It is recommended that audible noise generated by the terminal should be kept at a minimum at all times.

- 10.2.1.8 B The terminal shall neither in operation nor in standby emit noise to the ambient environment that causes damage or unintentional annoyance to the users or bystanders.
- 10.2.1.9 B The terminal shall, with e.g. possible fan working, comply with the noise limits defined in table 10.1.

Table 10.1 – Noise limits

	Category A	Category B	Category C
Equipment (in stand-by) switched on and off for printing or distribution	Below 50 dbA at 0.50 meters	Below 50 dbA at 0.50 meters	Below 50 dbA at 0.50 meters
Equipment in the process of printing or distribution	Below 60 dbA at 0.50 meters	Below 70 dbA at 1.00 meter	Below 70 dbA at 1.00 meter

### Thermal

Thermal design of the terminal shall be in accordance with the class of equipment and the environment in which it is installed. The terminal shall be able to operate in accordance with all other functional requirements within the limits specified.

Limits for storage without packing, with packing and in transport are out of the scope for this requirement specification and are solely defined by the Terminal Supplier.

- 10.2.1.10 A The terminal shall comply with the limits in operation for the categories A, B and C as defined in table 10.2.

Table 10.2 – Thermal requirements

	Category A	Category B	Category C
Temperature	+5°C to +40°C	-10°C to +50°C	-20°C to +50°C
Gradient max	10°C /hour	20°C /hour	20°C /hour
Relative humidity	20 á 80 % with condensation	20 á 80 % without condensation	15 á 95 % without condensation
Max humidity gradient	10 % /hour	10 % /hour	10 % /hour
Splash proofing			Protected against waterspray according to ref. 31: "EN 60 529". Resistant to frost and defrost
Atmospheric pressure	Maximum altitude 2000 meters	Maximum altitude 2000 meters	Maximum altitude 2000 meters

### Reliability

The terminal should be manufactured to a high standard of reliability in order to assure availability for payments at almost all times.

Failures caused by hardware or software malfunctions requiring the terminal to be corrected by the manufacturer or his representative should be kept to a minimum.

- 10.2.1.11 C The Mean Time Between Failures (MTBF) may provide an overall failure rate lower than .25 failures per terminal per year.

## 10.2.2 Combined Card Reader

- 10.2.2.1 B A CAT terminal shall have a combined card reader if magnetic stripe cards are supported.

- 10.2.2.2 C A POS terminal may have a combined card reader.

## 10.2.3 Integrated Circuit Card Reader

- 10.2.3.1 B The ICCR shall have landing contacts.

- 10.2.3.2 A The ICCR shall be able to connect to cards with physical characteristics in accordance with ref. 6: "ISO/IEC 7816-1".

- 10.2.3.3 A The ICCR shall be able to connect to cards with contacts placed in accordance with ref. 7: "ISO/IEC 7816-2".

- 10.2.3.4 B The ICCR shall have a service life comparable to the service life of the terminal which it is meant for.



- 10.2.3.5 A If the ICCR is not a motorized card reader, the card inserted shall be accessible for the user.
- 10.2.3.6 C The ICCR may contain a mechanism which is able to lock the inserted card during a payment sequence.
- 10.2.3.7 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.
- 10.2.3.8 A Physical removal of the inserted card at any time shall not leave the terminal in an invalid or unknown state.
- 10.2.3.9 A The inserted card shall be inserted with the short side first.
- 10.2.3.10 B The short side nearest the contacts shall be inserted first.
- 10.2.3.11 B The contacts of the card shall face the cardholder, when the card is inserted using the right hand.
- 10.2.3.12 A The ICCR shall be able to accept cards with the contacts on the same side as (possible) embossing.
- 10.2.3.13 B Active measures shall be taken in order to prevent the user from destroying the card reader e.g. by inserting coins.
- NOTE:** This can be done by narrowing the card slot or by equipping the card reader with a coin slot in the bottom. The card slot however, shall allow cards with embossing to be inserted, which gives a minimum slot of 1.27 mm according to ref. 2: “ISO/IEC 7810”.
- 10.2.3.14 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. 26: “EN 726–4”.
- 10.2.3.15 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. 26: “EN 726–4”.
- 10.2.3.16 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. 26: “EN 726–4”.

#### 10.2.4 Magnetic Stripe Card Reader

- 10.2.4.1 B The MSCR shall have a service life comparable to the service life of the terminal which it is meant for.
- 10.2.4.2 A The MSCR shall not damage any MSC swiped/inserted.
- 10.2.4.3 B The MSCR shall be a swipe–reader, manual insertion reader or be motorized.

- 10.2.4.4 C A ‘shutter’ may be installed to protect the MSCR against insertion of irrelevant material.
- 10.2.4.5 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.
- 10.2.4.6 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
- 10.2.4.7 B It shall be possible to operate the MSCR with either hand.
- 10.2.4.8 B If the MSCR is a separate swipe-reader, the MSCR shall be able to read the MSC when swiped in either direction.

### 10.2.5 PSAM Card Reader(s)

- 10.2.5.1 B The CAD shall have at least 4 PSAM Card Readers (PCRs).
- 10.2.5.2 C The PSAM Card Reader(s) may have landing contacts (sliding contacts are allowed).
- 10.2.5.3 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. 27: “ENV 1375-1” (ID-000 format).
- 10.2.5.4 A The PCR shall be able to connect to cards with contacts placed in accordance with ref. 7: “ISO/IEC 7816-2”.
- 10.2.5.5 B The PCR shall have a service life comparable to the service life of the terminal which it is meant for.
- 10.2.5.6 A Physical removal of the inserted PSAM at any time shall not leave the terminal in an invalid or unknown state.
- 10.2.5.7 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. 26: “EN 726-4”.
- 10.2.5.8 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. 26: “EN 726-4”.
- 10.2.5.9 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. 26: “EN 726-4”.

### 10.2.6 Merchant Application Interface

- 10.2.6.1 C The terminal may be able to connect to the Merchant Application by an 8 pin connector (“Bell-connector”) described in ref. 14: “ISO/IEC 8877”.

## 10.2.7 Visual Indicators

- 10.2.7.1 A The Cardholder Display shall, as an absolute minimum, be able to display two lines of text simultaneously.
- 10.2.7.2 B The Cardholder Display shall be able to display four lines of text simultaneously.
- 10.2.7.3 C The Cardholder Display may be able to display more than four lines of text simultaneously.
- 10.2.7.4 A Each line of text on the Cardholder Display shall be able to contain 16 characters simultaneously.
- 10.2.7.5 B Each line of text on the Cardholder Display shall be able to contain 20 characters simultaneously.
- 10.2.7.6 C Each line of text on the Cardholder Display may contain more than 20 characters.
- 10.2.7.7 A The Cardholder Display shall be alphanumeric.  
Display messages defined in this specification, or otherwise desired by the Terminal Supplier, may exceed  $4 \times 20$  characters.
- 10.2.7.8 B Messages exceeding the capability of the Cardholder Display shall be edited in co-operation with PBS.
- 10.2.7.9 A The Cardholder Display shall be able to show the digits: “0” – “9”.
- 10.2.7.10 A The Cardholder Display shall be able to show decimal numbers with two decimals.
- 10.2.7.11 A The Cardholder Display shall at least be able to show the capital letters: “A” – “Z”, and the Danish capital letters: “Æ”, “Ø”, and “Å”.
- 10.2.7.12 C The Cardholder Display may be able to show the lower case letters: “a” – “z”, and the Danish letters: “æ”, “ø”, and “å”.
- 10.2.7.13 C The Cardholder Display may be able to show other language specific letters.
- 10.2.7.14 B The character height of the Cardholder Display shall be at least 5.5 mm.
- 10.2.7.15 B LCD Cardholder Displays with a character height less than 6.5 mm shall be backlit (when in use).
- 10.2.7.16 B The Cardholder Display shall be readable in a viewing angle of at least  $\pm 30^\circ$  from perpendicular to the surface. See figure 10.2.

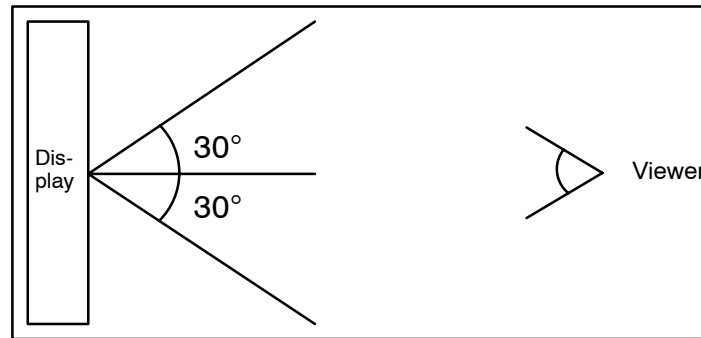


Figure 10.2 – Viewing angle

- 10.2.7.17 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.

**NOTE:** Addition information could be wallpaper.

- 10.2.7.18 A The Cardholder Display shall be easily readable under a wide range of lighting conditions encountered in retail environments.

For requirement 10.2.7.18, consideration should be given about the front, the size of characters and possible internal lightning as required in the individual installation to meet general ergonomic needs.

## 10.2.8 Audio Indicator

The functional requirements can be found in section 5.6.5.

- 10.2.8.1 B The terminal shall have an audible indicator to signal changes in its status during operation or to indicate depression of keys.
- 10.2.8.2 B If an audible signal is used, the signal shall not last more than 10 seconds.
- 10.2.8.3 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.
- 10.2.8.4 B After evaluating the transaction result, a tone of 440 Hz. +/- 5% shall be used to indicate the completion of a rejected/failed transaction.
- 10.2.8.5 A The two frequencies used to indicate a successful transaction and a rejected/failed transaction shall not be in any form of harmony.
- 10.2.8.6 B The duration of the approval tone shall be 150 milliseconds +/- 10 milliseconds.
- 10.2.8.7 B The duration of the rejection tone shall be 500 milliseconds +/- 10 milliseconds.

- 10.2.8.8 A The audio signals shall be given simultaneous with the corresponding visual indication.
- 10.2.8.9 B The volume of the audio indicator shall be adjustable.
- NOTE:** The audio volume may be controlled by means of hardware or software functions.
- 10.2.8.10 C It may be possible to suppress the audio indicator.

## 10.2.9 Cardholder Keyboard / Command Keys

### Cardholder Keyboard

- 10.2.9.1 A It shall be possible for the cardholder to clearly distinguish the Cardholder Keyboard/Keypad from the PIN Pad, i.e. the Cardholder Keyboard shall be marked differently from the PIN Pad.
- This is to prevent the cardholder from accidentally entering the PIN on the Cardholder Keyboard, with danger of the PIN being displayed in plaintext or even worse, “snatched” by a fraudster. See requirements H.2.2.1 to H.2.2.6.
- 10.2.9.2 C The keyboard may allow entry of alpha characters A–Z and Æ, Ø, Å and “space”.
- 10.2.9.3 C The keyboard may allow entry of alpha characters a–z and æ, ø and å.
- 10.2.9.4 A PBS shall approve the design and layout of the Cardholder Keyboard.

## 10.2.10 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

- 10.2.10.1 A PBS shall approve the design and layout of the PIN Pad.
- 10.2.10.2 A The numeric layout of the PIN Pad shall comply with ref. 36: “EMV, version 4.1”.

**NOTE:** Referring to requirement 10.2.10.2, an example is given in figure 10.3.

**NOTE:** The command keys are not part of the PIN Pad and need not be covered by a privacy shielding. It is, however, allowed to shield the command keys as well.

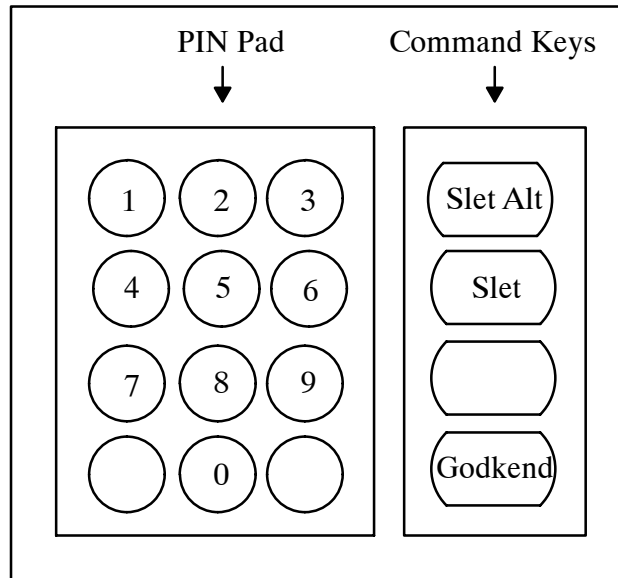


Figure 10.3 – PIN Pad and Command Key layout

- 10.2.10.3 A For PIN Pads supporting alphanumeric mapping in addition, the keyboard layout shall be according to ref. 57: “ECBS DEBS100”. Figure 10.4 shows the layout of alphanumeric keys.

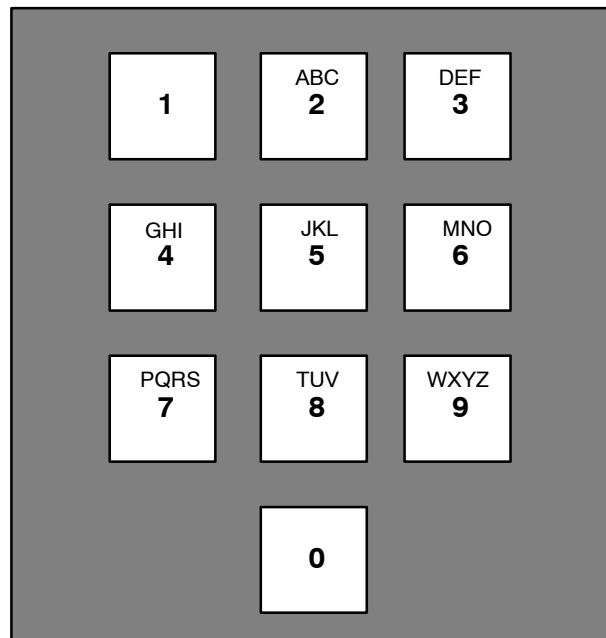


Figure 10.4 – Layout of Alphanumeric Keys

- 10.2.10.4 A Digits 1 and 0 shall not contain any alphabetic characters.

**PIN Privacy**

To prevent PINs 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.

- 10.2.10.5 A Requirements concerning the privacy shielding around the PIN Pad and the actual placing of the PIN Pad when installed are defined in Attachment H and shall be fulfilled.

### **General Requirements**

- 10.2.10.6 B The keyboard/keypad and the PIN Pad shall be designed to optimize the operation from an ergonomic point of view.
- 10.2.10.7 B The keyboard/keypad and the PIN Pad shall have a neutral surface and be non-reflecting with a good contrast to the keys.
- 10.2.10.8 A It shall be possible to operate any keyboard/keypad and the PIN Pad with both the left and the right hand.
- 10.2.10.9 A The key for “5” shall have a tactile identifier.
- 10.2.10.10 B The size of keys shall be min. 12 mm measured where the keys have the smallest length.
- 10.2.10.11 A The key movement for mechanical keys shall be 0.8–4.8 mm.
- 10.2.10.12 A The activation force for pressing a key shall be 0.25–1.5 N.
- 10.2.10.13 B At depression the key top shall be over or in level with the surface.
- 10.2.10.14 A The terminal shall only include one PIN Pad used for all key-entering of PIN-values.

### **General Hardware Requirements**

- 10.2.10.15 A A PIN Entry Device (PIN Pad) shall be a Secure Cryptographic Device as defined in ref. 16: “ISO 9564–1”.
- 10.2.10.16 A The Secure Cryptographic Device shall be so designed that it is not practical for a fraudster to construct a replica from commercially available components that can reasonably be mistaken for a genuine Secure Cryptographic Device.
- Monitoring attack shall be countered by using tamper resistant device characteristics.
- 10.2.10.17 A The PED shall be so designed as to preclude the addition of any kind of PIN tapping device.
- 10.2.10.18 A If the design requires that parts of the Secure Cryptographic Device be physically separate and processing data and/or cardholder instructions pass between these parts there shall be an equal level of protection among all parts of the Secure Cryptographic Device.

### **Tamper Evidence**

- 10.2.10.19 A The physical design shall be such that there will be a high degree of probability of detection of any modification or substitution.

- 10.2.10.20 A The Secure Cryptographic Device shall be so designed and constructed that any successful penetration shall require that the Secure Cryptographic Device be subjected to physical damage such that the Secure Cryptographic Device cannot be put back into service without a high probability of the tampering being detected.
- 10.2.10.21 A The Secure Cryptographic Device shall be so designed and constructed that any unauthorized additions to the Secure Cryptographic Device, intended to monitor it for sensitive data, shall have a high probability of being detected before such monitoring can occur.
- 10.2.10.22 A A Physically Secure Device shall be designed to restrict physical access to internally stored sensitive data and to deter theft, unauthorized use and modification.
- The above requirement normally requires incorporation of tamper –resistance, –evidence, –indication and/or –response mechanisms. These can be visible and/or audible alarms.
- 10.2.10.23 A A Physically Secure Device shall not contain sensitive information when it is not in use.

#### **Tamper Resistance**

- 10.2.10.24 A A Secure Cryptographic Device shall be so designed and constructed that any unauthorized access to or modification of sensitive data that are input, stored or processed in it shall necessitate physical penetration of the Secure Cryptographic Device.
- 10.2.10.25 A The Secure Cryptographic Device and its data entry functions shall be so shielded from direct and indirect monitoring that, when operated in its intended environment, no feasible attack will result in compromise of any secret or sensitive data.
- 10.2.10.26 A A Secure Cryptographic Device shall be Tamper Resistant to such a degree that its passive resistance is sufficient to make penetration infeasible both in its intended environment and when taken to a specialized facility.
- 10.2.10.27 A It shall require specialized skills and equipment to determine data stored within the Secure Cryptographic Device, to modify data and to re-install the Secure Cryptographic Device.
- 10.2.10.28 A Secure Cryptographic Devices shall be designed to withstand state-of-the-art monitoring attacks known at the time of certification, e.g. Differential Power Analysis and Timing Attack.

#### **Tamper Response**

- 10.2.10.29 A The Secure Cryptographic Device shall be designed to detect any unauthorized modification.



- 10.2.10.30 A The Secure Cryptographic Device shall be designed and constructed in such a way that penetration of the Secure Cryptographic Device results in the immediate and automatic erasure of all keys, other sensitive data and useful residues of sensitive data.
- 10.2.10.31 A If the security of the device depends on the operating environment, the unauthorized movement of the device shall cause the immediate and automatic erasure of all keys, other sensitive data and all useful residue of sensitive data.
- 10.2.10.32 B If a Secure Cryptographic Device is constructed/designed to permit access to internal areas for e.g. maintenance, it shall have a mechanism so that such access causes immediate erasure of all cryptographic keys and other sensitive data.
- NOTE:** If compromise of secret keys and other sensitive data can be prevented, the Secure Cryptographic Device need not erase secret keys and other sensitive data.
- 10.2.10.33 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.

### **PED Software**

**NOTE:** In addition to the security requirements to the PED hardware, firm requirements to the organizational conditions for development, installation, operation, and maintenance have been defined in section 10.4.3.

### **Command Keys**

- 10.2.10.34 B The color of the “SLET ALT” (Cancel) key shall be red.
- 10.2.10.35 B The color of the “SLET” (Clear) key shall be yellow.
- 10.2.10.36 B The color of the “GODKEND” (Enter/Accept) key shall be green.
- 10.2.10.37 C The lettering on the command keys may be colored instead of the key itself.
- 10.2.10.38 B The “SLET ALT” (Cancel), “SLET” (Clear) and “GODKEND” (Enter/Accept) keys shall be vertically arranged, located furthest to the right of the PIN Pad and with the following arrangement:
- The “SLET ALT” (Cancel) key shall be the uppermost key,
  - the “SLET” (Clear) key shall be in the middle and
  - the “GODKEND” (Enter/Accept) key shall be the lowest key.
- 10.2.10.39 C If the command keys are vertically arranged, an additional key may be mounted between the “SLET” (Clear) and the “GODKEND” (Enter/Accept) keys.

- 10.2.10.40 B If an additional key is mounted between the “SLET” (Clear) and the “GODKEND” (Enter/Accept) keys, then this key may be either without text (indicating no functionality) or with the text “INFO” (Information).
- 10.2.10.41 B If an additional “INFO” (Information) key is included, then the color of this key shall be blue.
- 10.2.10.42 C The lettering on the “INFO” (Information) key may be blue instead of the key itself.
- 10.2.10.43 C If the “SLET ALT” (Cancel), “SLET” (Clear) and “GODKEND” (Enter/Accept) keys are horizontally arranged the keys may be located on the bottom row of the keyboard with the following arrangement:
- The “SLET ALT” (Cancel) key shall be the left key,
  - the “SLET” (Clear) key shall be in the middle and
  - the “GODKEND” (Enter/Accept) key shall be the right key.
- 10.2.10.44 C If the “INFO” key is implemented, this key shall be placed between the “SLET” and the “GODKEND” keys.
- 10.2.10.45 A The terminal shall be equipped with an Eject Button.
- 10.2.10.46 B The Eject Button shall be red, if implemented as a dedicated button.
- NOTE:** The Eject Button does not have to be a dedicated button. The Eject Button may be activated by physically removing the card from the card reader.
- 10.2.10.47 B The size of command keys shall be 1.5 to 2 times bigger than keys on the PIN Pad.

### 10.2.11 Receipt Printer

- 10.2.11.1 B The Receipt Printer shall be capable of printing at least 24 alphanumeric characters per line.
- 10.2.11.2 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).

## 10.3 Electrical Design

### 10.3.1 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.

### 10.3.2 General Requirements

- 10.3.2.1 B When mains power is used a 230V+/-10% @ 50Hz supply shall be assumed for general purpose.
- 10.3.2.2 A The terminal shall not lose data due to power failure.
- 10.3.2.3 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.
- 10.3.2.4 C In the event of mains power failure, when the terminal is supplied by e.g. rechargeable batteries, it may be able to complete 10 to 50 transactions.

### 10.3.3 Electrical Safety

In order to protect the user and the terminal from electrical hazard the EC act on product liability applies to the terminal.

This includes protection provided by rules for e.g. electrical grounding, maximum electrical leakage, rigidity of cabling and connection, and thermal hazards.

- 10.3.3.1 A The terminal shall not cause any form of electrical shock.
- 10.3.3.2 A When mains power is used the terminal shall comply with ref. 32: “EN 60 950”.  
Requirement 10.3.3.2 is given by the authorities.
- 10.3.3.3 A When an internal modem is used in the terminal the hardware shall comply with ref. 28: “EN 41 003”.

### 10.3.4 Electromagnetic Compatibility

The terminal will be required to be able to work in an electrically noisy environment and adequate precautions need to be taken to ensure that misoperations do not occur due to either transient interference on mains supply (short duration spikes or voltage drops) or radiation sources (e.g. from fluorescent lighting or motors).

For immunity to electromagnetic interference generated by other equipment in the environment, the terminal shall comply with standards covering all classes of installation.

- 10.3.4.1 A The terminal shall comply with ref. 30: “EN 55 022”.

### 10.3.5 Circuit Design

- 10.3.5.1 A The terminal shall be equipped with a fuse in the power supply line.

- 10.3.5.2 A The terminal shall be able to withstand drop-outs in the power supply of 200 ms. The drop-out shall not influence the correct functioning of the terminal.
- 10.3.5.3 A The terminal shall be able to withstand voltage spikes in the power line of 1,000 Volts in 1 ms. The voltage spike shall not influence the correct functioning of the terminal.
- 10.3.5.4 A The terminal shall actively prevent that Cards are being damaged by static discharge when inserted.

### 10.3.6 Electrical Interfaces

#### PSAM

- 10.3.6.1 A The CAD shall be able to supply 50 mA @ 5 V  $\pm 5\%$  to each PSAM.
- 10.3.6.2 A The  $V_{PP}$  contact (C6) shall be electrically isolated (not connected).
- 10.3.6.3 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.
- 10.3.6.4 A The power supply to the PSAM shall be short circuit proof.
- 10.3.6.5 A The CAD shall be able to connect electrically to the PSAM in accordance with ref. 8: “ISO/IEC 7816-3” clause 5.1.
- 10.3.6.6 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.
- 10.3.6.7 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.
- 10.3.6.8 A The CAD shall be equipped with a pull-up resistor according to ref. 8: “ISO/IEC 7816-3”.
- 10.3.6.9 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.
- 10.3.6.10 A The CAD shall be able to handle the PPS dialog in accordance with ref. 8: “ISO/IEC 7816-3”.

**NOTE:** It is recommended that the CAD selects 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.

### Cards

- 10.3.6.11 A The CAD shall be able to supply 50 mA at 5 V  $\pm 5\%$  to the ICC.
- 10.3.6.12 A The  $V_{PP}$  contact (C6) shall be electrically isolated.
- 10.3.6.13 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.

- 10.3.6.14 A The power supply to the Card shall be short circuit proof.
- 10.3.6.15 A The CAD shall be able to connect electrically to the card in accordance with ref. 8: “ISO/IEC 7816–3”.
- 10.3.6.16 A The CTRL pin shall electrically comply with the values given in ref. 8: “ISO/IEC 7816–3” for the RST pin.
- 10.3.6.17 A No short circuit or damage shall take place when inserting or removing the card.
- 10.3.6.18 A The CAD shall be equipped with a pull–up resistor according to ref. 8: “ISO/IEC 7816–3”.
- 10.3.6.19 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.
- 10.3.6.20 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 .

**NOTE:** The CAD may increase the clock frequency after the ATR sequence.

- 10.3.6.21 A The CAD shall be able to handle the PPS dialog in accordance with ref. 8: “ISO/IEC 7816–3”.

**NOTE:** It is recommended that the CAD selects 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

- 10.3.6.22 A The protocol between the terminal and the Merchant Application is out of scope for this specification, but the following minimum requirements shall be fulfilled by the selected protocol.
- The protocol shall indicate if the transmission was successful (including at least 2–way handshake).

- A package shall be retransmitted at least 3 times if an unsuccessful response is received.
- A package shall be retransmitted at least 3 times if no response is received within a given time (2 times the maximum allowed response time of a successful response).
- A checksum shall be included in each package.

**NOTE:** A suggested protocol between the Merchant Application and CAD can be the XMODEM protocol.

- 10.3.6.23 C Data exchange between the terminal and the Merchant Application may be carried out using CCITT V.24, see ref. 34: “CCITT V.24”.
- 10.3.6.24 B The terminal shall operate as DTE (Data Terminal Equipment).
- 10.3.6.25 B The CCITT V.24 interface shall be able to withstand  $\pm 1200$  Volt relative to the GND pin of the terminal power supply.
- 10.3.6.26 B In order to reduce the communication time higher transmission speeds might be applicable in some configurations, e.g. direct communication to a computer. In this case the following transmission speeds are applicable: 9600 bits/s, 12000 bits/s, 19200 bits/s, 24000 bits/s, 38400 bits/s, 76800 bits/s and 115200 bits/s.

### 10.3.7 Data Store

The speed of the Data Store is very important for the overall transaction time.

- 10.3.7.1 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.

## 10.4 Software Design

### 10.4.1 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).

### 10.4.2 General Requirements

- 10.4.2.1 B The software that handles payments and the related user interface in the terminal shall be developed in a modular way for easier maintenance.

**NOTE:** E.g. the software consists of separate modules of 1–2 A4 page(s) of source-code each with one function de-

scribed with input– and output–parameters and their usage.

- |          |   |   |
|----------|---|---|
| 10.4.2.2 | B | The software shall be developed using structured analysis, design, and test.  |
| 10.4.2.3 | A | The software modules shall be under configuration management.   |
| 10.4.2.4 | A | It shall be possible to add and update/modify, in a secure manner, from a Terminal Operator each application software module. |
| 10.4.2.5 | A | No parts of the software shall contain self–modifying code.   |
| 10.4.2.6 | B | No (or only small) part(s) of the software shall be made in assembly language.  |
| 10.4.2.7 | A | Access to the terminal kernel shall be restricted.  |
| 10.4.2.8 | A | The terminal shall be able to compute the Terminal Checksum according to the data element definition in section 9.2.79.       |

### 10.4.3 Additional Requirements to the PED Software

The security required for handling PINs is not only dependent on selection of the appropriate algorithms and procedures but also on the correct implementation in hardware and software. Equally important is that the security components in all phases of development, installation and operation are protected against undetected changes.

This adds requirements to:

- the development process
- the implementation and maintenance processes,
- the installation, as well as
- the operation

#### Development Process

- |          |   |   |
|----------|---|---|
| 10.4.3.1 | A | The manufacturer shall document that the development model has at least the following three (or equivalent) steps: <ul style="list-style-type: none"> <li>• Functional specification</li> <li>• Software architecture, and</li> <li>• Detail specification</li> </ul> |
| 10.4.3.2 | A | The security relevant components and interfaces as well as their border to not security relevant components shall be fully documented and available for security audit.   |
| 10.4.3.3 | A | The documentation shall be protected against unauthorized access and especially against undetected changes during definition, storing, transfer, archiving and review.  |

### **Implementation and Maintenance**

- 10.4.3.4 A The software implementation shall be performed in a structured manner such that the security components and interfaces defined in the detail specification can be clearly identified.
- 10.4.3.5 A The software shall be written in a well documented programming language.
- 10.4.3.6 A The source code shall be readily available for inspection or security audit.
- 10.4.3.7 A The manufacturer shall document that the source code during implementation and maintenance is fully under version control and change management.
- 10.4.3.8 A The manufacturer shall document that the resources responsible for the implementation are aware of their responsibilities and have their access rights fully defined.
- 10.4.3.9 A The manufacturer shall document that the implementation and maintenance are conducted in an environment and with tools sustaining the auditability of the process.
- 10.4.3.10 A The manufacturer shall perform extensive tests of functionality as well as security.
- 10.4.3.11 A The manufacturer shall especially document that the intended function cannot be abused or circumvented and that only the intended functions can be performed.
- 10.4.3.12 A The manufacturer shall document all test data and test events.
- 10.4.3.13 A The manufacturer shall keep the documentation readily available for audit purposes.
- 10.4.3.14 A The manufacturer shall document that necessary maintenance, replacement and updating of components are organized and conducted in a way that prevents unauthorized changes to devices and programs in a credible manner.
- 10.4.3.15 A Subsequent upload of security related components shall only take place after mutual cryptographic authentication of the parties involved.
- 10.4.3.16 A The integrity of program updates shall be protected.

### **Installation**

- 10.4.3.17 A The manufacturer shall define installation procedures for all components and related tools so the terminal/PED and the software are protected against undetected manipulation all the way from implementation to operation.



## Audit

As it is not possible to secure a system completely, the most important security function is to recognize attacks and attempts on attack. Furthermore, the overall system security functions shall support analysis of attacks and necessary alarm handling and counter measures. Also, misdeeds from normally authorized personnel shall as a minimum be discovered and proven. To support this, audit trails and logs are necessary.

In the logs, the breach of security regulations and irregularities in the system (e.g. incorrect release, multiple initializations of individual system components) shall be recorded. These records shall be maintained in a way that it is possible to reconstruct operations performed with sensitive data and the results. The records shall be maintained to an extent that leads to relevant handling within an acceptable time frame.

- |           |   |  |
|-----------|---|--|
| 10.4.3.18 | A | The manufacturer shall document the implemented level and detail of logging.   |
| 10.4.3.19 | A | All breaches of security regulations, irregularities in systems, and attempts to fraud as well as actions taken shall be recorded.         |
| 10.4.3.20 | A | All data needed to reconstruct the breach shall be logged.   |
| 10.4.3.21 | A | Logged data shall be readily available that counter measures towards security breaches and irregularities can be taken in a timely manner. |
| 10.4.3.22 | A | Logged data shall be protected against unauthorized access, unauthorized manipulation and erasure.   |

## Handling of Alarms

In the case where an attack on the system is detected, an alarm shall be triggered. For all defined alarms, a responsible entity shall be assigned as well as which counter measures and defence strategies to apply. Also, procedures to establish the damage shall be in place.

This is especially true for the compromising of encipherment keys and PINs. In order to detect such as fast as possible alarms shall be triggered whenever signs of compromising of either keys or PINs, e.g. damaged or temporarily missing security modules, delayed delivery of keys, failing integrity test, are observed/detected.

- |           |   |  |
|-----------|---|--|
| 10.4.3.23 | A | The manufacturer shall document on which conditions an alarm shall be triggered. Based on these conditions, the necessary information to trigger the alarm shall be defined. The required logging shall fulfill the requirements as defined in 10.4.3.2. |
| 10.4.3.24 | A | All defined alarms shall include:  |

- Who is responsible for reacting on the alarm
  - Procedures for finding the level of damage
  - Recovery procedures and counter measures to apply
  - Reaction time: immediately or later
- 10.4.3.25 A The following alarm shall exist:
- Whenever a key is compromised at creation, distribution, storing, or during operation

#### 10.4.4 Data Management

##### Application Independent Data Management

- 10.4.4.1 A The Data Store shall contain an area of at least 64 Kbytes for update commands for the PSAM.
- 10.4.4.2 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

- 10.4.4.3 A The Data Store shall contain an area for update commands for software modules.

#### 10.4.5 Storage of Data

##### Terminal Data

- 10.4.5.1 A The memory used for storage of non-transient data shall be non-volatile.
- 10.4.5.2 B The memory used for storage of data shall be able to keep data for 5 years without power.

##### PIN Pad Data

- 10.4.5.3 A The memory used for storage of non-transient data shall be non-volatile.
- 10.4.5.4 B The memory used for storage of data shall be able to keep data for 10 years without power.
- 10.4.5.5 A The PIN Pad ID shall be stored in non-volatile memory inside the PIN Pad.
- 10.4.5.6 A It shall be possible to load the PIN Pad ID at the PIN Pad manufacturer site before shipping the PIN Pad.
- 10.4.5.7 A It shall not be possible to change the PIN Pad ID once it has been loaded.

## 10.4.6 Storage of Software

### Terminal Software

- |          |   |   |
|----------|---|---|
| 10.4.6.1 | A | The actual software version no. shall be stored in the terminal.  |
| 10.4.6.2 | A | The actual software version shall be stored in an electronic media and it shall be possible to show it on the Cardholder Display. |
| 10.4.6.3 | A | The actual hardware version no. shall be stored in the terminal.  |
| 10.4.6.4 | A | The actual hardware version shall be stored in an electronic media and it shall be possible to show it on the Cardholder Display. |
| 10.4.6.5 | A | The software shall be kept in non-volatile memory, e.g. PROM/EPROM/EEPROM, flash-PROM or diskette.                                |
| 10.4.6.6 | B | The memory shall be able to keep data for 5 years without power.  |

### PIN Pad Software

- |           |   |   |
|-----------|---|---|
| 10.4.6.7  | A | The actual software version no. shall be stored in the PIN Pad.   |
| 10.4.6.8  | A | The actual software version shall be stored in an electronic media and it shall be possible to show it on the Cardholder Display. |
| 10.4.6.9  | A | The actual hardware version no. shall be stored in the PIN Pad.   |
| 10.4.6.10 | A | The actual hardware version shall be stored in an electronic media and it shall be possible to show it on the Cardholder Display. |
| 10.4.6.11 | A | The software shall be kept in non-volatile memory, e.g. PROM/EPROM/EEPROM or flash-PROM.  |
| 10.4.6.12 | B | The memory shall be able to keep data for 5 years without power.  |

## 10.4.7 Download Requirements

- |          |   |  |
|----------|---|--|
| 10.4.7.1 | A | It shall only be possible for <i>either</i> the Terminal Supplier <i>or</i> the Terminal Operator to update the applications stored in the terminal.   |
| 10.4.7.2 | A | The Terminal Supplier <i>or</i> the Terminal Operator shall be able to update the operating system, parameters and the application(s) in the terminal. |

- 10.4.7.3 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 these updated data elements to the MAD-Handler.

#### **Terminal Software Modules**

- 10.4.7.4 A Each module shall be upgradeable.
- 10.4.7.5 A Each update shall affect the software version stored in the terminal.
- 10.4.7.6 A The software download shall never be able to put the terminal out of business.
- 10.4.7.7 A No update shall be able to corrupt any data memory currently in use.
- 10.4.7.8 A The terminal shall ensure that the complete software update is loaded before switching to the new code.
- 10.4.7.9 A The download shall handle communication errors. This means that data errors during transmission shall result in data being retransmitted.
- 10.4.7.10 B The code to be downloaded shall be enciphered.

#### **PIN Pad Software**

- 10.4.7.11 A Downloading of program updates shall only take place after mutual cryptographic authentication of the communicating parties.
- 10.4.7.12 A Public key algorithm based on RSA shall be used to authenticate the downloaded software on the terminal.

A specific technique for authentication of the software must be implemented. This technique shall assure that only software produced by the supplier, owner or a third party approved by the controller can be loaded and installed in the Secure Cryptographic Device.

**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.

- 10.4.7.13 A PSAM application update commands shall be saved in the same memory area as other data update commands to the PSAM.

## 10.5 Network Design

### 10.5.1 Integration Between Terminal and Cash Register

The principle where a terminal and a cash register are connected physically and logically in the relationship 1-to-1 as depicted in figure 10.5, offers the best service seen from the cardholders perspective.

In the same way, it minimizes the risk of creating confusion in case of two or more cardholders wanting to perform a transaction at the same time.

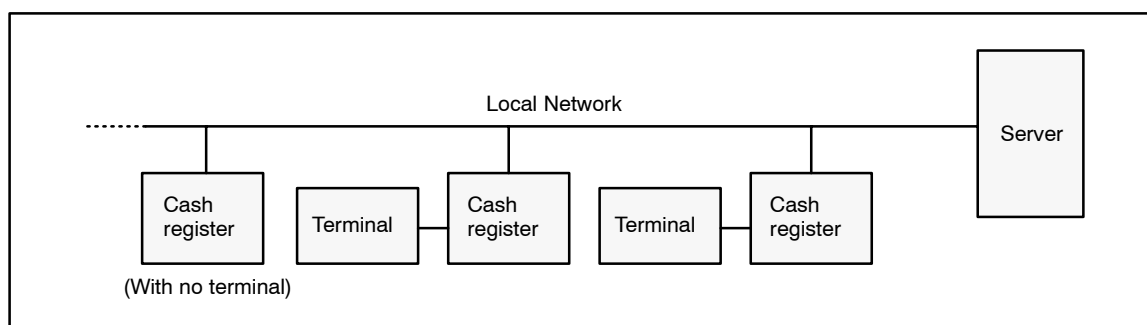


Figure 10.5 – Terminal and Cash Register Integration

- 10.5.1.1 A The POS terminal shall always be placed next to a cash register. That way, a direct contact between the merchant and cardholder is assured during a payment session. By placing the terminal next to the cash register it makes it easier for the merchant to hand over the receipt to the cardholder.

### 10.5.2 Network Connection

A connection between a number of terminals and a cash register system as shown in figure 10.6, may potentially introduce a risk of mixing up information between the cash registers and the logically connected terminals. The terminal interface must offer an opportunity to address a single unit on the local network.

Another aspect is the up-time of the local network. The POS terminal will depend on the up-time of the network as the terminals are 100 % dependent of the communication via the network.

The facility, where a single cash register is able to continue its tasks when the network is 'down', cannot be used if the customer wishes to pay with a card.

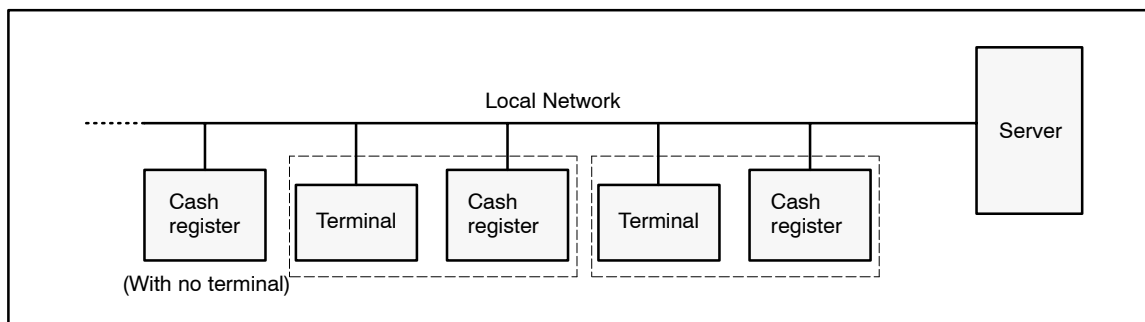


Figure 10.6 – Network Connection

- 10.5.2.1 A If a Terminal Supplier wants to implement a system using the above given principles, the Terminal Supplier shall assure that the logical connection between the units is sufficient and ensure that neither corruption nor mix-up of the data transmitted can take place.
- 10.5.2.2 A The Terminal Supplier shall also assure that the up-time of the local network in practice will be 100 %. This means that customers using Payment Cards will not be more poorly treated than other customers, measured on availability.
- 10.5.2.3 A If the terminal architecture is based on a distributed design i.e. a network is used for the communication between handlers, the design shall be accepted by PBS.

**NOTE:** It shall not be possible to eavesdrop the communication between handlers. Especially IP and wireless communication have the card schemes attention.

### 10.5.3 One Terminal Integrated with Several Cash Registers

- 10.5.3.1 A System solutions based on sharing of *one* POS terminal between two or more cash registers shall not be accepted.

The reason for this is the high probability that such a solution will introduce doubt or even disputes between cardholders concerning who is the next in line to be served.

A solution based on sharing of one POS terminal will introduce a risk of confusion, which, in some cases, might lead to one cardholder paying for another's goods.

# 11. Service Packs

## 11.1 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.

## 11.2 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 6.1.3 (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.

### 11.2.1 Terminal – Terminal Approval No.

In the data element Terminal Approval No., the 3 most significant bits is now used as Service Pack No.

- 11.2.1.1      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 9.2.78 (Data Elements).

## 11.3 Service Packs Overview

Table 11.1 show the relationship between Service Packs and commands, data elements & functions.

Table 11.1 – 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' <sup>1)</sup>	●	●	●
	'0008'			●
Set Debit/Credit Properties				
Identifier	'8000'			●
	'8001' – '8002' <sup>1)</sup>	●	●	●
Functionality				
MSC PIN retry			●	●
Issuer Envelope Data				●
Account Type				●
Message size (up to 512 bytes)		●	●	
Message size (up to 1024 bytes)				●
<b>Legend:</b>				
<sup>1)</sup> = Earlier versions of the PSAM may not be able to respond successfully to all identifier values.				

## 11.4 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 exiting command *Get Amount*.
- *Validate Data 2*, a new and extended variant of the exiting command *Validate Data*.



Service Pack No. 1 will also enable the use of the function “PIN Retry”.

#### 11.4.1 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 6.18.6 (Host Declined Transactions (Requests)).

#### 11.4.2 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 generate 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.

- 11.4.2.1 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 6.18.11.3, the Merchant Interface shall insert the Response Code 'FFF2' in *all* subsequent responses to *Get Amount 2* command.

See table 11.2 for comparison of the different variations of the *Get Amount* command.

### 11.4.3 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 CodePRINT:** 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 F.79 on page F-68 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'.

## 11.5 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.

### 11.5.1 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/cashregister 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/cashregister system, making it possible to compute the accurate amount.

When the PSAM request the final amount, the terminal/cashregister system shall return the accurate amount, otherwise the transaction will be rejected.

See table 11.2 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.

### 11.5.2 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. 41: "TAPA Errata".

Table 11.2 – 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	<b>Get Amount</b>	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	<b>Get Amount 2</b>	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	<b>Get Amount 3</b>	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.

### 11.5.3 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').

#### 11.5.4 Initiate Payment 2 / Account Type

The purpose of the data element Account Type is stated in ref. 36: “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.

- 11.5.4.1      A      The value shall be set to the default value ('00') until further notice.

# Attachment A. Magnetic Stripe Formats

## A.1 Introduction

### A.1.1 Track 2 Structure

The general structure of track 2 of the magnetic stripe as defined by ref. 3: “ISO/IEC 7811–2”, ref. 4: “ISO/IEC 7812–1” and ref. 5: “ISO/IEC 7813” is shown in table A.1.

Table A.1 – Track 2 Structure

Track 2 Structure			
Field	Length (4-bit)	Description	Value
1	1	Start Sentinel	'B'
2	11 – 19	PAN (Primary Account Number)	
3	1	Separator	'D'
4	4	Expiry Date (YYMM)	
5	3	Service Code	
6	0 – 18	Discretionary Data	
7	1	End Sentinel	'F'
8	1	Longitudinal Redundancy Check	

## A.2 Credit/Debit Cards

The format for the national debit card with ICC (“Dankort”) is shown in table A.2.

Table A.2 – Magnetic Stripe Contents of a Dankort

Dankort			
Field	Length (4-bit)	Description	Value
1	1	Start Sentinel	'B'
2	4	First four digits of PAN (Primary Account Number)	'5019'
3	4	Registration No.	
4	6	Card Serial No.	
5	1	Check digit 1 (modulo 11)	
6	1	Check digit 2 (modulo 10)	
7	1	Separator	'D'
8	4	Expiry Date (YYMM)	
9	3	Service Code	'601'
10	1	Discretionary Data	
11	6	Discretionary Data	
12	1	Discretionary Data	
13	2	Discretionary Data	
14	2	PI Card Type	'50' – '54'
15	1	Discretionary Data	
16	1	End Sentinel	'F'
17	1	Longitudinal Redundancy Check	



The format for the combined international and national debit card with ICC (“Visa/Dankort”) is shown in table A.3.

Table A.3 – Magnetic Stripe contents of a Visa/Dankort

Visa/Dankort			
Field	Length (4-bit)	Description	Value
1	1	Start Sentinel	‘B’
2	4	First four digits of PAN (Primary Account Number)	‘4571’
3	4	Registration No.	
4	6	Card Serial No.	
5	1	Check digit 1 (modulo 11)	
6	1	Check digit 2 (modulo 10)	
7	1	Separator	‘D’
8	4	Expiry Date (YYMM)	
9	3	Service Code	‘201’
10	1	Discretionary Data	
11	6	Discretionary Data	
12	1	Discretionary Data	
13	2	Discretionary Data	
14	2	PI Card Type	‘40’ – ‘44’
15	1	Discretionary Data	
16	1	End Sentinel	‘F’
17	1	Longitudinal Redundancy Check	

This page is intentionally left blank

# Attachment B. Validation of the PAN (Primary Account Number)

## B.1 Check Digit Modulus 10

### B.1.1 Modulus 10 Calculation

All cards conforming to ref. 4: “ISO 7812–1” will, as part of the PAN (Primary Account Number), include a check digit. The check digit is the least significant digit.

**NOTE:** Only selected digits from the PAN in the magnetic stripe may be embossed/printed on the card. Consequently, additional information about the card may be necessary for key entering the PAN.

- B.1.1.1 A The check digit shall be calculated on the preceding digits of the entire PAN and shall be calculated according to the Luhn formula for modulus 10 check digit.

**NOTE:** The check digit will be verified by the PSAM.

### B.1.2 Luhn Formula for Calculating Modulus 10 Check Digit

The following steps are involved in this modulus 10 “double–add–double” calculation:

Step 1: Double the value of alternate digits beginning with the first right hand digit (low order).

Step 2: Add the individual digits comprising the products obtained in Step 1 to each of the unaffected digits in the original number.

Step 3: Subtract the total obtained in Step 2 from the next higher number ending in 0, (this is the equivalent of calculating the “tens compliment” of the low order digit (unit digit) of the total). If the total obtained in Step 2 is a number ending in zero (30, 40, etc.), the check digit is 0.

Table B.1 – Example using Luhn formula to calculate modulus 10 check digit

Example:																	
Identification number without check digit														Check digit	Step		
5	0	1	9	2	0	0	0	2	0	3	8	7	1	5		1	
x2		x2		x2		x2		x2		x2		x2		x2			
10		2		4		0		4		6		14		10			
1+0+0+2+9+4+0+0+0+4+0+6+8+1+4+1+1+0 = 41															2		
50 – 41 = 9															3		
Identification number with check digit																	
5	0	1	9	2	0	0	0	2	0	3	8	7	1	5	9		

### B.1.3 Modulus 10 check digit verification

Verification of the check digit involve the following steps:

Step 1: Double the value of alternate digits beginning with the *second* right hand digit.

Step 2: Add each individual digits calculated in Step 1 to each of the unaffected digits.

Step 3: Divide the total obtained by ten. The result shall leave no remainder (no decimals).

Example (from above):

Identification number including the check digit (**9**):

5019 2000 2038 7159

1+0+0+2+9+4+0+0+0+4+0+6+8+1+4+1+1+0+**9**=50 Step 2

Verification: 50/10 = 5 (no remainder)

Step 3

# Attachment C. SDL Notation

## C.1 Introduction

SDL is described in detail in ref. 35: “CCITT Z.100” but the subset used for this specification is briefly explained in the following pages. This should make all the diagrams understandable to the reader.

An SDL specification defines a system consisting of a number of processes, where each process is a state machine with a number of states and a number of variables. When a process is in a stable state, it is able to receive a signal. Depending on the signal received, different transitions can be followed to a new state.

A transition consists of a number of tasks to be executed and signals to be sent. The precise tasks to be executed and signals to be sent can be guided by decisions based on the contents of the variables.

When a transition is terminated, a new stable state is reached.

## C.2 Symbols and their Meaning

### Start Symbol

The starting point of a process is represented by the symbol:

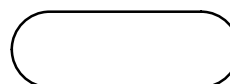


Figure C.1 – Start Symbol

The start symbol must be followed by a transition, which is immediately executed when the process is started.

### State

A stable State is represented by the symbol:

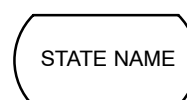


Figure C.2 – Symbol for a State

When a process is in a stable state it is ready to accept signals. During a transition from one state to another all signals will be ignored.

The possible inputs in a certain state may not all be shown on the same diagram. When several diagrams are used to define a certain state, the meaning is as if the two diagrams were merged.

Several states can be defined simultaneously by putting the names of all the states to be defined in the state symbol. A '\*' in a state means all states, except states that are local to a procedure.

When a transition terminates in a state named '-', it means that that state machine goes to the state in which it was when the transition was initiated.

### Input

An Input is represented by the symbol:

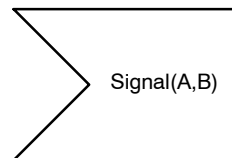


Figure C.3 – Symbol for Input signals

The meaning of an input is that when a process receives a signal then the corresponding input is executed, and the data attached to the signal are assigned to the variables in the input.

The input may be a wildcard input, indicated by a '\*' in the input symbol. A wildcard input will handle all signals not explicitly handled by other inputs. Any data carried by such a signal are lost.

After the input is executed, the transition following it is executed until a new state is reached.

### Task

A Task is represented by the symbol:

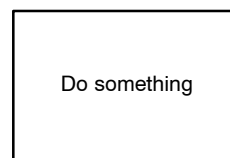


Figure C.4 – Symbol for a Task

The meaning of a task is to do what is described inside it. A task is not detailed further in other diagrams.

### Output

An Output is represented by the symbol:

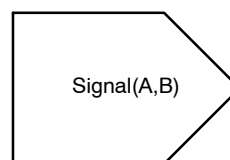


Figure C.5 – Symbol for Output signals

The meaning of an output is that the signal carrying the values given by the expressions is sent out.

### Decision

A Decision is represented by the symbol:

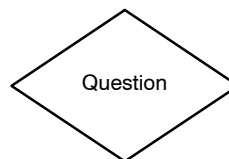


Figure C.6 – Symbol for a Decision

A decision allows a transition to branch. The answer to the question can be either yes or no. Which path to follow in the two situations will be indicated by the letters Y (for yes) and N (for no).

### Join / Label

A Join/Label is represented by the symbol:

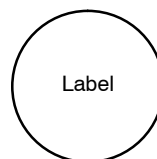


Figure C.7 – Symbol for a Label

If a transition ends in a join, execution will continue from the place where the corresponding label is found.

### Stop

A stop is represented by the symbol:

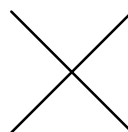


Figure C.8 – Symbol for a Stop

If a transition ends in a stop symbol, the process terminates.

### Macro

An application of a Macro is represented by the symbol:

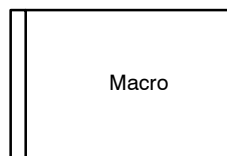


Figure C.9 – Symbol for a Macro

A macro is described in more detail on another diagram. The meaning of an application of a macro is, as if the application is replaced by the definition of the macro.

In some situations there can be several ways out of a macro (typically **Success** and **Error**). In such cases each path out is labelled in order to remove ambiguities.

### Procedure

An application of a procedure is represented by the symbol:

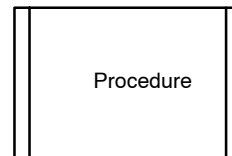


Figure C.10 – Symbol for a Procedure

The body of a procedure is defined on another diagram.

The starting point of a procedure is defined by the symbol:

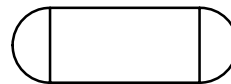


Figure C.11 – Procedure Start Symbol

Termination of the procedure is represented by the symbol:

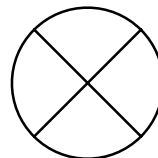


Figure C.12 – Symbol for the Termination of a Procedure

The meaning of a procedure call is to behave as given by the procedure body, starting at the procedure start symbol, until a termination symbol is reached. In contrast to a macro, a procedure only has one way in and one way out. Furthermore, states defined in the body of a procedure are local to the procedure.



# Attachment D. Certification



The certification process is described in a separate document.

This page is intentionally left blank

# Attachment E. Cardholder Activated Terminals

## E.1 Introduction

Cardholder Activated Terminals is the designation for payment terminals which the cardholder operates without an Attendant present. An Automated Teller Machine (ATM) is not considered to be a CAT.

In order to counter the enhanced risk of fraud with an electronic payment without a human factor to assess the security, the acquirer and the Card Acceptor shall observe more rigorous rules for certification, surveillance, functions and documentation for such equipment. The Card Acceptor and the acquirer shall furthermore assume a greater responsibility for the risk involved and inform the Issuer of which type of terminal and level is used when performing transactions. The same terminal may have different levels depending on which card or function is used or depending on the amount.

As a general rule, the requirements for the different CAT levels are the same.

Development of a CAT terminal shall not be initiated unless in agreement with PBS.

## E.2 CAT Levels

Cardholder Activated Terminals are grouped into four different levels:

- level 1 – Automated Dispensing Machines,
- level 2 – Self-Service Terminals,
- level 3 – Limited Amount Terminals and
- level 4 – In-Flight Terminals.

Specific additional requirements for the various CATs are defined below.

Visa categorizes acceptance devices by the types of transactions they process. Transaction categories are based on risk level.

- **Type A Transactions** – Are less than U.S.\$40, or local currency equivalent. Type A transactions are not authorized, and cardholder verification is not performed.
- **Type B Transactions** – Are less than U.S.\$100, or local currency equivalent. Type B transactions are authorized, but cardholder verification is not performed.
- **Type C Transactions** – Are not limited to any dollar amount. Type C transactions are authorized and PIN verification is required.

Additional requirements given in ref. 44: “M/Chip Functional Architecture – For Debit and Credit” and ref. 43: “Visa Integrated Circuit Card. Terminal Specification” must be followed.

## E.2.1 CAT Level 1 – Automated Dispensing Machines

CAT Level 1 – Automated Dispensing Machines are unattended, online capable terminals that operate with a zero floor limit. This CAT must support PIN.

- E.2.1.1 A An Automated Dispensing Machines shall *not* dispense cash.
- E.2.1.2 A An Automated Dispensing Machines shall be capable of conveying the following information to the cardholder:
- Card invalid for this service
  - Service unavailable now
  - Invalid PIN – re-enter
  - Card retained (if it is able to retain cards)
  - Produce a transaction receipt
- E.2.1.3 C For ICCs, the Automated Dispensing Machine may support PIN verification in both online and offline environments.
- E.2.1.4 A If the Automated Dispensing Machine is able to retain cards, the retained card shall be logged.

## E.2.2 CAT Level 2 – Self-Service Terminals

CAT Level 2 – Self-Service Terminals are unattended, online capable terminals that operate with a zero floor limit for limited amount transactions. No CVM is required.

- E.2.2.1 A A Self-Service Terminal shall authorize all transactions.
- E.2.2.2 A A Self-Service Terminal shall produce a transaction receipt upon cardholders request.
- E.2.2.3 A A Self-Service Terminal shall *not* dispense cash.

## E.2.3 CAT Level 3 – Limited-Amount Terminals

CAT Level 3 – Limited Amount Terminals are unattended terminals with no online capability accepts limited amount transactions. No CVM is required.

- E.2.3.1 B A Limited-Amount Terminal shall check the PAN against a negative file for authorization, if the terminal is able to retain this information.
- E.2.3.2 A A Limited-Amount Terminal shall produce a transaction receipt, except for MSC telephones.
- E.2.3.3 A A Limited-Amount Terminal shall *not* dispense cash.

## E.2.4 CAT Level 4 – In-Flight Terminals

CAT Level 4 – In-Flight Terminals are payment terminals operated by either the cardholder or the flight personnel. No CVM is required.

# Attachment F. Host Communication for the Debit/Credit Application – Protocols and Formats

## F.1 Introduction

This attachment defines the communication with the Terminal Operator host when performing debit/credit transactions.

The message formats are based on ref. 38: “APACS Standard 60”.

The notation used in this attachment is defined in section 3.2.3.

## F.2 General

In this attachment, 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 Call Numbers

To ensure the highest level of accessibility to the PBS platforms for online authorization and advice transfer, dual access points are established for the involved platforms.

The device making the connection to PBS (the CAD or terminal server depending on the network topology) is responsible for using both the primary and secondary access point.

## F.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 F.1.

Table F.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, ...

### F.3.1 Physical Layer

- F.3.1.1 B The physical layer may either be a switched network (e.g. PSTN, ISDN or GSM) or a permanent network (e.g. GPRS or ADSL).
- F.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).
- F.3.1.3 A It shall be possible to update both set of address parameters.
- F.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 PBS platform.

**NOTE:** When the network transfers the A-number to the PBS platform, the host systems will be able to identify the terminals address on the network.

### **F.3.2 Data Link Layer**

F.3.2.1 A The data link layer shall use PPP.

The assigned IP addresses will be without authenticity and consequently there is no use of neither PAP nor CHAP.

### **F.3.3 Network Layer**

F.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.

### **F.3.4 Transport Layer**

F.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.

F.3.4.2 C Mapping of the terminal entity to the TCP address may be performed either in software or in a router.

### **F.3.5 Session Layer**

The session layer carries the authorization transactions, the financial notifications, etc.

### **F.3.6 Presentation and Application Layers**

The presentation and application layers are specified in the remaining part of this attachment.

F.3.6.1 A The communication interface shall be able to send and receive messages of a size up to at least 1K bytes.

## **F.4 Transmission Flows**

The transmission flows for the different debit/credit transaction types are described in chapter 6 (Debit/Credit Functionality).

## F.5 Transmission Formats

### F.5.1 APACS Message Types

Table F.2 lists the APACS message types used in the OTRS environment.

Table F.2 – APACS Message Types used in OTRS

ISO	MTI	Message Type	Source	Transaction Type/Process
1100	0106	Authorization Request	PSAM	Original 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 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
1304	0370	File Action Instruction Ack.	CAD	
1420	0426	Reversal Advice	PSAM	Reversal (Authorization) Purchase (failed) Refund (failed) Original 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
–	0805	Network Management Request Repeat	CAD	
–	0814	Network Management Request Response	Host	
–	0844	Network Management Notification	CAD/Host	

### F.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 F.3 defines the first byte.

**NOTE:** Multiple occurrences of a data object shall not appear.

Table F.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

- F.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 F.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 F.4 – List of Data Objects for use in the APACS Header

Tag	Attrib.	Length	Comment
'C0'	b2	2	Length of the following <sup>1)</sup> 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, excl. length field)
'C4'	n6	3	Systems Trace Audit Number (identical to field 11 if this is present)
'C5'	b1	1	KEK <sub>DATA</sub> version (key version for key using to encipher KSES <sub>DATA</sub> )
'C6'	b16	16	[KSES <sub>DATA</sub> ] (enciphered key for APACS 60 message)
'C7'	b1	1	APACS MAC Key version
'C8'	n3	2	Advice Window Size
'C9'	b1	1	Advice Request Flag
'CA'	..ansp20	..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: <sup>1)</sup> 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.

- F.5.2.2 A Depending on the value of L its length may be 1, 2 or 3 bytes as defined in table F.5. The shortest possible form shall always be selected.

Table F.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 F.7.

### General APACS Message with Header

Table F.6 defines the general format for an APACS Message including the APACS Header.

Table F.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 F.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).

- F.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 F.7.

Table F.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

- F.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.

- F.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 F.7.12).
- F.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 F.7.12).
- 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 PBS.

F.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 F.13 for the definition of the data elements.

**NOTE:** The communication interface is the interface responsible for the TCP/IP communication with PBS according to Tag 'CB' (Network Connection Type).

**NOTE:** Requirement F.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.

F.5.2.8 A The CAD shall include all mandatory data objects defined in table F.8 in the APACS Header when sending a self–generated message to the host.

Table F.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
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.

F.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 F.9 will be included in the APACS Header sent by the host.

- F.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 F.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	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	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	–	N/A	–	–	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	–	–	–	–	–	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 F.10.

Table F.10 – Example of an APACS Message with Header

Field name	Tag	Attrib.	Length	Value (hex) including Tag, Length
Protocol type	–	an3	3	<b>41 36 30</b> (“A60”)
Protocol version	–	an1	1	<b>31</b> (“1”)
APACS Header, type 0	‘E0’	–	var.	<b>E0 5B</b> (Header length = 91)
Length of APACS msg.	‘C0’	b2	2	<b>C0 02 00 E6</b> (Length = 230)
Message Type Identifier	‘C1’	an4	4	<b>C1 04 30 31 30 36</b> (MTI=“0106”)
APACS MAC Key Version	‘C7’	b1	1	<b>C7 01 0A</b> (Key# 10)
KEK <sub>DATA</sub> Version	‘C5’	b1	1	<b>C5 01 04</b> (Key# 4)
[KSES <sub>DATA</sub> ]	‘C6’	b16	16	<b>C6 10 94 74 5D EA 75 4F 01 AB 76 9A 33 CA 67 3A DF 8B</b> (enciphered key)
Function Code	‘C2’	n4	2	<b>C2 02 01 01</b> (101: Original authorization, estimated amount)
Terminal Identification	‘CD’	an8	8	<b>CD 08 54 45 52 4D 30 30 30 39</b> (“TERM0009”)
STAN	‘C4’	n6	3	<b>C4 03 01 79 64</b> (STAN = 17964)
MAD–Handler ID	‘CC’	ans8	8	<b>CC 08 31 32 33 34 35 36 37 38</b> (= “12345678”)
Communication Interface Statistics	‘CF’	–	var.	<b>CF 08 12 34 56 78 9A BC DE F0</b> <sup>1)</sup>
PSAM Identifier	‘C3’	b13	13	<b>C3 0D A0 00 00 01 20 00 00 00 05 03 95 6A 56</b> RID <sub>PSAM</sub> = ‘A00000120’ (PBS Data) ID <sub>PSAMCREATOR</sub> = 5 ID <sub>PSAM</sub> = 60123734 (‘03956A56’)
Network Connection Type	‘CB’	b1	1	<b>CB 01 00</b> (0: Terminal directly connecting to PBS)
APACS message	–	–	–	<b>92 8A 65 82 ...</b> (arbitrary example showing an enciphered message) This examples assumes a total length of 230 bytes for the enciphered APACS message.

NOTE: <sup>1)</sup> The length of 8 bytes is just an example.

## F.6 Communication Statistics and Error Counters

### F.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.

### F.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.

### F.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).

- F.6.3.1      A      The terminal shall have error counters for (at least) the following errors (see table F.11):
- No response from PBS (no of time-outs)
  - Card Reader error (Magnetic stripe and ICC)
  - Unsupported cards
  - Communication errors between the CAD and the Merchant Application
- F.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 F.13.

Table F.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 PBS (number of time-outs) Card reader errors Unsupported cards Communication errors with the Merchant Application

### F.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**

- F.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**

- F.6.4.2 A When reading a MSC, the counter for tag ‘TF’ shall be incremented when the conditions in requirement 5.5.2.10 have been fulfilled.

- F.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**

- F.6.4.4 A When reading a MSC, the counter for tag ‘TG’ shall be incremented when the conditions in requirement 5.13.4.5 have been fulfilled.

- F.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**

- F.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.

## F.7 Primitive Data Objects for the APACS Header

This subsection defines the coding of primitive data objects for use in the APACS Header.

### F.7.1 Coding of Tag 'C0' (Length of APACS 60 Message)

F.7.1.1 A The value field for Tag 'C0' shall be coded on two bytes binary.

### F.7.2 Coding of Tag 'C1' (Message Type Identifier)

F.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. 15: "ISO/IEC 8859-15".

### F.7.3 Coding of Tag 'C2' (Function Code)

F.7.3.1 A The value field for Tag 'C2' shall be coded as defined in section F.9.6.

### F.7.4 Coding of Tag 'C3' (PSAM Identifier)

F.7.4.1 A The value field for Tag 'C3' shall be coded as defined in section F.9.15 (without the length field required when transmitted in field 60).

### F.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.

### F.7.6 Coding of Tag 'C5' (KEK<sub>DATA</sub>)

F.7.6.1 A This data object (Tag 'C5') shall never be inserted by the CAD.

### F.7.7 Coding of Tag 'C6' ([KSES<sub>DATA</sub>])

F.7.7.1 A This data object (Tag 'C6') shall never be inserted by the CAD.

### F.7.8 Coding of Tag 'C7' (APACS MAC Key Version)

F.7.8.1 A This data object (Tag 'C7') shall never be inserted by the CAD.

### F.7.9 Coding of Tag ‘C8’ (Advice Window Size)

- F.7.9.1 A This data object (Tag ‘C8’) shall never be inserted by the CAD.
- F.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.

### F.7.10 Coding of Tag ‘C9’ (Advice Request Flag)

- F.7.10.1 A This data object (Tag ‘C9’) shall never be inserted by the CAD.
- F.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 for Advice Transfer/PSAM Update.

‘01’: The CAD is requested to perform an Advice Transfer followed by the PSAM Update process.

- F.7.10.3 A When Tag ‘C9’ is received and the value indicates that Advice Transfer 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 Advice Transfer/PSAM update sequence, no message needs to be displayed.

### F.7.11 Coding of Tag ‘CA’ (Display Line for Host Message)

- F.7.11.1 A This data object (Tag ‘CA’) shall never be inserted by the CAD.
- F.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 frontend 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. 15: “ISO/IEC 8859–15”. The length is variable up to 20 bytes.

- F.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.

### F.7.12 Coding of Tag ‘CB’ (Network Connection Type)

- F.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 F.12 shall be used.

Table F.12 – Coding of the Network Connection Type

Value	Meaning
'00'	The transaction is generated in a stand-alone terminal with its own PBS PSAM. The terminal is directly connected to the transmission line.
'01'	The transaction is generated in a terminal with its own PBS 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 PBS.
'02'	The transaction is generated in a terminal without a PBS PSAM. The terminal is connected to a terminal server (via a public or private network) hosting one or more PBS PSAMs. The terminal server enables multiple terminals to share one or more transmission lines to PBS.
'03'..'FF'	RFU

### F.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.

### F.7.14 Coding of Tag 'CD' (Terminal Identification)

F.7.14.1 A This data object (Tag 'CD') shall never be inserted by the CAD.

### F.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.

### F.7.16 Coding of Tag 'CF' (Communication Interface Statistics)

This data object ('CF') is reserved for communication interface statistics.

F.7.16.1 A The format of the Statistic Vector shall be according to table F.13.

The error counters and statistics are also defined in table F.13.

F.7.16.2 A When a message from PBS 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.

F.7.16.3 A If the Connection Request counter reach the maximum value (65535), the incrementing of this counter shall stop.

- F.7.16.4 A If the Connection Time counter reach the maximum value (4.294.967.295), the incrementing of this counter shall stop.
- F.7.16.5 A If a Connection Error counter reach the maximum value (255), the incrementing of this counter shall stop.

### F.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 Attachment N “Guidelines for Constructing Total Reports” for further details.

### F.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 F.13 – Communication Interface – Statistic Vector

Field	Field Name	Attrib.	Value	Comments	Connection Type <sup>1)</sup>	
					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 PBS 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 PBS	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 <sup>2)</sup>	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" <sup>3)</sup>	M	M

**Legend:** M = Mandatory, O = Optional, if not provided set to '00'.

<sup>1)</sup> See definition in field 4.

<sup>2)</sup> 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.

<sup>3)</sup> The host is closing the connection after 30 seconds without any valid transactions (non-activity time-out).

## F.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.

## F.8.1 Authorization Request Messages (0106/0116)

Table F.14 – Authorization Request – ICC (Original 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.	<b>Present if field 35 is absent</b>
3	Processing code		n6		3	See section F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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	<b>Present if field 35 is absent</b> (From Tag '5F24')
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
23	Card sequence number		n3		2	<b>If present on ICC</b>
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
30	Amount, original transaction		n12		6	<b>If Supplementary Authorization.</b>
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	ans ..255		var.	<b>Present if Online PIN.</b> See section F.9.12
49	Currency code, transaction		n3		2	
52	PIN data		b8		8	<b>Present if Online PIN.</b> Enciphered PIN block
55	ICC system related data	LLVAR	b ..MAX		var.	See section F.9.13
56	Original data elements	LVAR	b ..32		26	<b>If Supplementary Authorization.</b> Echo from 0106–message: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	



Table F.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	
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	<b>If transaction is approved</b>
39	Action code		n4		2	See section F.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
55	ICC system related data	LLVAR	b ..MAX		var.	<b>Present if data received from Issuer.</b> See section F.9.13
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0106–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section F.9.18
64	Message authentication code		b8		8	

Table F.16 – Authorization Request – MSC (Original 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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
30	Amount, original transaction		n12		6	<b>If Supplementary Authorization.</b>
35	Track 2 data	LVAR	z ..37		var.	
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.	<b>Present if Online PIN.</b> See section F.9.12
49	Currency code, transaction		n3		2	
52	PIN data		b8		8	<b>Present if Online PIN.</b> Enciphered PIN block
56	Original data elements	LVAR	b..32		26	<b>If Supplementary Authorization.</b> Echo from 0106–message: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table F.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	
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	<b>If transaction is approved</b>
39	Action code		n4		2	See section F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0106–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section F.9.18
64	Message authentication code		b8		8	

Table F.18 – Authorization Request – Key Entered (Original 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.	
3	Processing code		n6		3	See section F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
30	Amount, original transaction		n12		6	<b>If Supplementary Authorization.</b>
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	ans ..255		var.	See section F.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b..32		26	<b>If Supplementary Authorization.</b> Echo from 0106–message: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table F.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	<b>If transaction is approved</b>
39	Action code		n4		2	See section F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0106–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section F.9.18
64	Message authentication code		b8		8	

## F.8.2 Authorization Advice Messages (0126/0136)

Table F.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.	<b>Present if field 35 is absent</b>
3	Processing code		n6		3	See section F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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	<b>Present if field 35 is absent</b>
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
23	Card sequence number		n3		2	<b>If present on ICC</b>
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.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 F.9.13
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0126–message
61	Random number	LVAR	ansb ..255		9	Echo from 0126–message <b>Only if advice can be deleted from Data Store</b>

Table F.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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	
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
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0126–message
61	Random number	LVAR	ansb ..255		9	Echo from 0126–message <b>Only if advice can be deleted from Data Store</b>

Table F.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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.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	ans ..255		var.	See section F.9.12
49	Currency code, transaction		n3		2	'0000', if no currency is specified
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0126–message
61	Random number	LVAR	ansb ..255		9	Echo from 0126–message <b>Only if advice can be deleted from Data Store</b>

### F.8.3 Financial Request Messages (0206/0216)

Table F.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.	
3	Processing code		n6		3	See section F.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	
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3	200	2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	<b>Tag '57' if present in ICC</b>
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	
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.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	<b>If transaction is approved</b>
39	Action code		n4		2	See section F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0206–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section F.9.18
64	Message authentication code		b8		8	

Table F.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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3	200	2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	
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.	<b>Present if Online PIN.</b> See section F.9.12
49	Currency code, transaction		n3		2	
52	PIN data		b8		8	<b>Present if Online PIN.</b> Enciphered PIN block
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAM</sub> CREATOR    ID <sub>PSAM</sub>
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	

Table F.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	<b>If transaction is approved</b>
39	Action code		n4		2	See section F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0206–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section F.9.18
64	Message authentication code		b8		8	

Table F.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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3	200	2	See section F.9.6
25	Message reason code		n4		2	See section F.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	ans ..255		var.	See section F.9.12
49	Currency code, transaction		n3		2	
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
62	Merchant Initiative	LVAR	ansb ..255		2	See MI in "Data Elements"
64	Message authentication code		b8		8	



Table F.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	<b>If transaction is approved</b>
39	Action code		n4		2	See section F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0206–message
63	PSAM Updates	LLVAR	ansb ..MAX		var.	See section F.9.18
64	Message authentication code		b8		8	

## F.8.4 Financial Advice Messages (0226/0236)

Table F.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.	<b>Present if field 35 is absent</b>
3	Processing code		n6		3	See section F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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	<b>Present if field 35 is absent</b>
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
23	Card sequence number		n3		2	<b>If present on ICC</b>
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
30	Amount, original transaction		n12		6	<b>Only present if field 4 is different from 0106–message</b>
35	Track 2 data	LVAR	z ..37		var.	<b>Tag '57' if present in ICC</b>
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if authorized against Acquirer host</b>
39	Action code		n4		2	See section F.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
49	Currency code, transaction		n3		2	
55	ICC system related data	LLVAR	b ..MAX		var.	See section F.9.13
56	Original data elements	LVAR	b ..32		26	<b>Present if authorized:</b> Echo from 0106–message: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.33 – 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 F.9.9
41	Card accepting device id.		an8		8	Echo from 0226–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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message <b>Only if advice can be deleted from Data Store</b>

Table F.34 – Financial Advice – ICC (Refund)

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.	<b>Present if field 35 is absent</b>
3	Processing code		n6		3	See section F.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	<b>Present if field 35 is absent</b>
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3	200	2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	<b>Tag '57' if present in ICC</b>
37	Retrieval reference number		anp12		12	Batch number
39	Action code		n4		2	See section F.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
49	Currency code, transaction		n3		2	
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.35 – Financial Advice Response – ICC (Refund)

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 F.9.9
41	Card accepting device id.		an8		8	Echo from 0226–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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message <b>Only if advice can be deleted from Data Store</b>

Table F.36 – 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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
30	Amount, original transaction		n12		6	<b>Only present if field 4 is different from 0106–message</b>
35	Track 2 data	LVAR	z ..37		var.	
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if authorized against Acquirer host</b>
39	Action code		n4		2	See section F.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
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b ..32		26	<b>Present if authorized:</b> Echo from 0106–message: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.37 – 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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message <b>Only if advice can be deleted from Data Store</b>

Table F.38 – 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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
30	Amount, original transaction		n12		6	<b>Only present if field 4 is different from 0106–message</b>
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if authorized against Acquirer host</b>
39	Action code		n4		2	See section F.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	ans ..255		var.	See section F.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b ..32		26	<b>Present if authorized:</b> Echo from 0106–message: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.39 – 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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0226–message
61	Random number	LVAR	ansb ..255		9	Echo from 0226–message <b>Only if advice can be deleted from Data Store</b>

## F.8.5 PSAM Update Messages (0360/0370)

Table F.40 – 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 F.9.6
27	Download control		n6		3	See section F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
63	PSAM update	LLVAR	ansb ..MAX		var.	See section F.9.18

Table F.41 – 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 F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>

**This page is intentionally left blank**

## F.8.6 Reversal Advice Messages (0426/0436)

Table F.42 – 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.	<b>Present if field 35 is absent</b>
3	Processing code		n6		3	See section F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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	<b>Present if field 35 is absent</b>
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
23	Card sequence number		n3		2	<b>If present on ICC</b>
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	<b>Tag '57' if present in ICC</b>
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if Authorization Response was received</b>
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	
55	ICC system related data	LLVAR	b ..MAX		var.	See section F.9.13
56	Original data elements	LVAR	b ..32		26	Echo from 0106/0226-msg.: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.43 – 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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426–message
61	Random number	LVAR	ansb ..255		9	Echo from 0426–message <b>Only if advice can be deleted from Data Store</b>

Table F.44 – 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.	<b>Present if field 35 is absent</b>
3	Processing code		n6		3	See section F.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	<b>Present if field 35 is absent</b>
15	GMT offset		n3		2	See section F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	<b>Tag '57' if present in ICC</b>
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if Authorization Response was received</b>
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	
56	Original data elements	LVAR	b ..32		26	Echo from 0106/0226–msg.: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.45 – 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 F.9.9
41	Card accepting device id.		an8		8	Echo from 0426–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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426–message
61	Random number	LVAR	ansb ..255		9	Echo from 0426–message <b>Only if advice can be deleted from Data Store</b>

Table F.46 – 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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
35	Track 2 data	LVAR	z ..37		var.	
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if Authorization Response was received</b>
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	
56	Original data elements	LVAR	b..32		26	Echo from 0106/0206/0226–msg.: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.47 – 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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426–message
61	Random number	LVAR	ansb ..255		9	Echo from 0426–message <b>Only if advice can be deleted from Data Store</b>

Table F.48 – 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 F.9.2
4	Amount, transaction		n12		6	
8	Cashback amount		n12		6	<b>Only present if cashback</b>
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 F.9.3
21	POS capability code		an6		6	See section F.9.4
22	POS entry mode		n6		3	See section F.9.5
24	Function code		n3		2	See section F.9.6
25	Message reason code		n4		2	See section F.9.7
37	Retrieval reference number		anp12		12	Batch number
38	Approval code		anp6		6	<b>Present if Authorization Response was received</b>
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	ans ..255		var.	See section F.9.12
49	Currency code, transaction		n3		2	
56	Original data elements	LVAR	b..32		26	Echo from 0106/0206/0226–msg.: See section F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
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 F.49 – 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 F.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
60	PSAM identifier	LVAR	ansb ..255		14	Echo from 0426–message
61	Random number	LVAR	ansb ..255		9	Echo from 0426–message <b>Only if advice can be deleted from Data Store</b>

## F.8.7 Addendum Record Messages (0624/0634)

Table F.50 – 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 F.9.6
25	Message reason code		n4		2	See section F.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 F.9.14
60	PSAM identifier	LVAR	ansb ..255		14	RID <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
61	Random number	LVAR	ansb ..255		9	
71	Message number		n8		4	See section F.9.19
72	Data record	LLVAR	ansb ..MAX		var.	See section F.9.20
128	Message authentication code		b8		8	

Table F.51 – 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 F.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 <b>Only if advice can be deleted from Data Store</b>

## F.8.8 Service Record Messages (0624/0634)

Table F.52 – 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	2	See section F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
61	Random number	LVAR	ansb ..255		9	
64	Message authentication code		b8		8	

Table F.53 – 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 F.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 <b>Only if advice can be deleted from Data Store</b>

## F.8.9 Clock Synchronization Messages (0804/0814)

Table F.54 – 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 F.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number

Table F.55 – 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 F.9.3
39	Action code		n4		2	See section F.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number

## F.8.10 Installation Messages (0804/0814)

Table F.56 – Network Management Request – Installation

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 F.9.4
24	Function code		n3	880	2	See section F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
64	Message authentication code		b8		8	

Table F.57 – Network Management Request Response – Installation

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 F.9.3
39	Action code		n4		2	See section F.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	

## F.8.11 Advice Transfer Messages (0804/0814)

Table F.58 – 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 F.9.6
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number

Table F.59 – 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 F.9.3
39	Action code		n4		2	See section F.9.9
46	CAD management/service quality data	LVAR	ansb ..255		var.	At least: MAD–Handler ID Terminal Approval Number



## F.8.12 PSAM Update Messages (0804/0814/0844)

Table F.60 – 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 F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>

Table F.61 – 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 F.9.3
39	Action code		n4		2	See section F.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–message

Table F.62 – 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 F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>

### F.8.13 PSAM Deactivation Messages (0804/0814)

Table F.63 – 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 F.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 <sub>PSAM</sub>    ID <sub>PSAMCREATOR</sub>    ID <sub>PSAM</sub>
64	Message authentication code		b8		8	

Table F.64 – 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 F.9.3
39	Action code		n4		2	See section F.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.	<b>May be present</b> See section F.9.18

## F.9 Coding of Application Specific Fields

### F.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
- 63: PSAM Updates
- 72: Addendum Record

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
I1	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).

### F.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 1–2 are used (position 3–6 are set to zero).

Table F.65 – Applicable values for Field 3 (Processing Code).

Value	Description
<b>00xxxx–19xxxx</b>	<b>Debits</b>
000000	Goods and services
010000	Cash
020000	Adjustment
090000	Goods and services with cashback
110000	Quasi-cash and scrip
<b>20xxxx–29xxxx</b>	<b>Credits</b>
200000	Returns/Refunds
220000	Adjustment

### F.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 F.66 – 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 6.16.9, “Clock Synchronization”.

### F.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 F.84.

Position 1 defines the *primary* card data input capability.

Table F.67 – 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

Position 2 defines the *primary* cardholder authentication capability.

Table F.68 – 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 F.69 – 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 F.70 – 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 F.71 – 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 F.72 – 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, four different sets of POS Capability Codes are defined. These sets are named “Flex Terminal Capability Mark I – IV”.

Table F.73 – 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 F.74 – 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

Table F.75 – Flex Terminal Capability Mark II

Flex Terminal Capability Mark II		Terminal with PIN Pad, but without ICC reader
Position	Value	Description
1	2	Primary card data input: Magnetic stripe
2	1	Primary cardholder authentication: PIN
3	2 or 3	Card capture: 2 = No, 3 = Yes
4	1	Card data output: None
5	4	Print and Display: General
6	C	PIN capture: 12 digits

Table F.76 – Flex Terminal Capability Mark I

Flex Terminal Capability Mark I		Terminal without PIN Pad and ICC reader
Position	Value	Description
1	2	Primary card data input: Magnetic stripe
2	0	Primary cardholder authentication: No electronic authentication
3	2 or 3	Card capture: 2 = No, 3 = Yes
4	1	Card data output: None
5	4	Print and Display: General
6	0	PIN capture: No PIN capture capability

### F.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 F.83 and F.84.

Position 1 defines the operating environment.

Table F.77 – 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	CAT level 2 – no PIN – online only
9	CAT level 3 – no PIN – offline

Position 2 defines the cardholder presence.

Table F.78 – Applicable values for Field 22 (POS Entry Mode), position 2

Value	Description
0	Cardholder present
1	Cardholder not present, unspecified
2	Cardholder not present, mailorder
3	Cardholder not present, telephone order
5	Fallback processing

Position 3 defines the card data input mode.

Table F.79 – Applicable values for Field 22 (POS Entry Mode), position 3

Value	Description
0	Unspecified
2	Magnetic stripe read
5	ICC
6	Key entered
7	Magnetic stripe read after ICC malfunction

Position 4 defines the cardholder authentication mode.

Table F.80 – 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)



Position 5 defines the cardholder authentication entity.

Table F.81 – 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

Position 6 defines the CAD output status.

Table F.82 – 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

F.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 F.83.

**NOTE:** Additional information related to the MTI can be found in table F.84.

Table F.83 – POS Entry Mode Values to be Inserted in the *Initiate Payment* Command

Terminal Environment	Card Data Source				
	ICC	MSC		Key Entered	Token
		MSC	MSC (fallback)		
Attended	10500X	10200X	10700X	10600X	10000X
Mail order				12600X	12000X
Telephone order				13600X	13000X
CAT level 1	20500X	20200X	20700X		20000X
CAT level 2	80500X	80200X	80700X		80000X
CAT level 3	90500X	90200X	90700X		90000X

**Legend:** Coding of the POS Entry Mode. Position 1 is the leftmost position, position 6 the rightmost.  
X = don't care.

Table F.84 – Valid Values for POS Capability Codes and POS Entry Mode

				ISO 8583				APACS 60		
Environment	CVM	MTI	Transaction	POS Data Code				POS Capability Code, field 21:	POS Entry Mode, field 22:	
<b>ICC</b>										
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	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 F.84 – Valid Values for POS Capability Codes 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:	
<b>ICC</b>										
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	
<b>MSC</b>										
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	
	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	

Table F.84 – Valid Values for POS Capability Codes and POS Entry Mode (*continued*)

Environment	CVM	MTI	Transaction	ISO 8583				APACS 60	
				POS Data Code				POS Capability Code, field 21:	POS Entry Mode, field 22:
<b>MSC</b>									
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
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	J01	110	5 0 X 3 4 0	9 0 2 0 0 X
		0226	Not authorized	50X	O01	J01	110	5 0 X 3 4 0	9 0 2 0 0 X
<b>MSC (Fallback)</b>									
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	
	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	

Table F.84 – Valid Values for POS Capability Codes and POS Entry Mode (*concluded*)

				ISO 8583				APACS 60		
Environment	CVM	MTI	Transaction	POS Data Code				POS Capabili- ty Code, field 21:	POS Entry Mode, field 22:	
<b>MSC (Fallback)</b>										
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	

**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.

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.

## F.9.6 Coding of Field 24 (Function Code)

The following table defines the applicable values for this system.

Table F.85 – Applicable values for Field 24 (Function Code)

Value	Description
<b>100–199</b>	<b>Used for message types 01XX</b>
100	Original authorization. Amount accurate
101	Original authorization. Amount estimated
106	Supplementary authorization. Amount accurate
107	Supplementary authorization. Amount estimated
<b>200–299</b>	<b>Used for message types (01XX) and 02XX</b>
200	Original financial request/advice
201	Previously approved authorization. Amount same
202	Previously approved authorization. Amount differs
<b>300–399</b>	<b>Used for message types 03XX</b>
300	Unassigned
<b>400–499</b>	<b>Used for message types 04XX</b>
400	Full reversal. Transaction did not complete as approved
401	Partial reversal. Transaction did not complete for full amount
<b>600–699</b>	<b>Used for message types 06XX</b>
680	Addendum record
690	Service record
<b>800–899</b>	<b>Used for message types 08XX</b>
851	Exchange control, give token
852	Clock synchronization
880	Installation
882	Advice transfer
884	PSAM update
886	PSAM deactivation

## F.9.7 Coding of Field 25 (Message Reason Code)

The following table defines the applicable values for this system.

Table F.86 – Applicable values for Field 25 (Message Reason Code)

Value	Description
<b>1000–1499</b>	<b>Reason for an advice message rather than a request message</b>
1000	Not available
1003	Acquirer unavailable
1004	CAD (PSAM) processed
1005	ICC processing
1006	Under floorlimit
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)
<b>1500–1999</b>	<b>Reason for a request message rather than an advice message</b>
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
<b>4000–4999</b>	<b>Reason for a reversal</b>
4000	Customer cancellation
4001	Unspecified, no action taken
4003	Format error, no action taken
4007	CAD (PSAM) unable to complete transaction
4021	Time-out waiting for response
4204	ICC decline
<b>6000–6999</b>	<b>Reason for an administrative advice</b>
6000	Hotel
6001	Airlines
6002	Car rental

**NOTE:** The value 1151 is used for storing backup versions of advices in the Merchant Application.

### F.9.8 Coding of Field 27 (Download Control)

This 6-character field consists of two subfields. 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 F.87 – 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

### F.9.9 Coding of Field 39 (Action Code)

This 4-digit field consists of three individually coded subfields.

The following tables define the applicable values for this system.

Position 1 defines the immediate action to take.

Table F.88 – 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 6.18 on page 6-153

Position 2 defines any subsequent action to take.

Table F.89 – 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 F.90 – Action Codes – Applicable Values

Value	ASW	Description	Source	
			Host	PSAM
0000	'0000'	No further details	○	
0001	'12BA'	Honour with identification	○	
0002	'12BB'	Approved for partial amount	○	
0003	'1010'	Approved (VIP)	○	
0007	'1011'	Approved, update ICC	○	
0060	'1012'	Account service–limit–alarm (National use)	○	
0061	'1013'	Card service–limit–alarm (National use)	○	
0062	'12F0'	Loyalty card – approved (National use)	○	
0063	'1014'	Approved but suspected fraud (National use)	○	
0064	'1015'	Approved without financial impact (National use)	○	
0065	'1016'	Approved but not authorized by issuer (National use)	(○)	○
1000	'1200'	No further details	○	
1001	'1240'	Expired card	○	
1002	'1270'	Suspected fraud	○	
1003	'12B0'	Card acceptor contact acquirer	○	
1004	'1201'	Restricted card	○	
1005	'12B1'	Card acceptor call acquirer's security department	○	
1006	'12C0'	Allowable PIN tries exceeded	○	
1007	'12B2'	Refer to card issuer	○	
1008	'12B3'	Refer to card issuer's special conditions	○	
1009	'12D0'	Invalid merchant	○	
1010	'1250'	Invalid amount	○	
1011	'12E0'	Invalid card number	○	
1112	'1220'	PIN data required	○	
1013	'12B4'	Unacceptable fee	○	
1014	'12B5'	No account of type requested	○	
1015	'12B6'	Requested function not supported	○	
1016	'12B7'	Not sufficient funds	○	
1017/1117	'1221'	Incorrect PIN	○	
1018	'12E1'	No card record	○	
1019	'1310'	Transaction not permitted to cardholder	○	
1020	'1311'	Transaction not permitted to terminal	○	
1021	'1260'	Exceeds withdrawal amount limit	○	
1022	'12B8'	Security violation	○	
1023	'1290'	Exceeds withdrawal frequency limit	○	
1024	'1312'	Violation of law	○	
1025	'1232'	Card not effective	○	

Table F.90 – Action Codes – Applicable Values (*continued*)

Value	ASW	Description	Source	
			Host	PSAM
1026	'1280'	Invalid PIN block	○	
1027	'1281'	PIN length error	○	
1028	'1282'	PIN key synchronization error	○	
1029	'1271'	Suspected counterfeit card	○	
1060	'12B9'	Invalid date (National use)	○	
1061	'1203'	RFU (National use)	○	
1062	'120C'	Unable to locate previous message (National use)	○	
1063	'120D'	Data are inconsistent with original data (National use)	○	
1064	'1230'	Card entry found, but below low-range (National use)	○	
1065	'1231'	PAN-length not according to table-entry (National use)	○	
1066	'1202'	Cancellation cannot be accepted (National use)	○	
1067	'1300'	Match on previous transaction (National use)	○	
2000	'1500'	No further details (Pick up)	○	
2001	'1501'	Expired card (Pick up)	○	
2002	'1502'	Suspected fraud (Pick up)	○	
2003	'1503'	Card acceptor contact acquirer (Pick up)	○	
2004	'1504'	Restricted card (Pick up)	○	
2005	'1505'	Card acceptor call acquirer's security department (Pick up)	○	
2006	'1506'	Allowable PIN tries exceeded (Pick up)	○	
2007	'1507'	Special conditions (Pick up)	○	
2008	'1508'	Lost card (Pick up)	○	
2009	'1509'	Stolen card (Pick up)	○	
2010	'150A'	Suspected counterfeit card (Pick up)	○	
5000	'1618'	No host response received		○
5303	'1601'	Re-enter transaction	○	○
5304	'1602'	Format error	○	○
5316	'160C'	MAC incorrect	○	○
5406	'1603'/ '1020'/ '1618'	Cutover in process	○	
5407	'1604'/ '1020'	Card issuer or switch inoperative	○	
5408	'1605'	Transaction destination cannot be found for routing	○	
5409	'1606'	System malfunction	○	
5410	'1607'/ '1020'	Card issuer signed off	○	
5411	'1608'/ '1020'	Card issuer timed out	○	

Table F.90 – Action Codes – Applicable Values (*concluded*)

Value	ASW	Description	Source	
			Host	PSAM
5412	'1609'/ '1020'	Card issuer unavailable	○	
5414	'160A'	Not able to trace back to original transaction	○	
5415	'160B'/ '1020'	Reconciliation cutover or checkpoint error	○	
5417	'160D'	MAC key synchronization error	○	
5418	'160E'	No communication keys available for use	○	
5419	'160F'	Encryption key synchronization error	○	
5420	'1611'	Security software/hardware error – try again	○	
5421	'1612'	Security software/hardware error – no action	○	
5423	'1613'	Request in progress	○	
5445	'1614'/ '1020'	Host time-out (Private use)	○	
5484	'1615'	No valid conversion for a field value (National use)	○	
6002	'1780'	Invalid transaction	○	
6005	'1770'	Acquirer not supported by switch	○	
6013	'17A0'	Duplicate transmission	○	
6022	'17A1'	Message number out of sequence	○	
6050	'17A2'	Violation of business arrangement (National use)	○	
8000	–	Accepted/Successful	○	
8001	–	Accepted, unspecified mismatch in data	○	
8002	–	Accepted, format error (e.g. MAC error)	○	
8003	–	Accepted, card data mismatch	○	
8004	–	Accepted, merchant data mismatch	○	
8005	–	Accepted, PSAM ID mismatch	○	
8020	–	Rejected	○	
8421	–	Rejected, try again later	○	
8022	–	Rejected, format error (e.g. MAC error)	○	
8023	–	Rejected, card data mismatch	○	
8024	–	Rejected, merchant data mismatch	○	
8025	–	Rejected, PSAM ID mismatch	○	

### F.9.10 TLV Coding of Field 44 (Additional Response Data)

This field is TLV coded according to the definition in section F.9.1.

The applicable data objects are listed in the following table.

Table F.91 – 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 F.92
A4	Card Reconciliation Counter Name	ans16	Example of values are listed in table F.92
A5	Card Name (for printing)	ans16	Example of values are listed in table F.93
T1	Authorisation Response Code	an2	See ref. 11: "ISO 8583:1987" & ref. 36: "EMV, version 4.1"
TY	Issuer Envelope Response Data	..b150	At the Issuer discretion

Table F.92 – 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 F.93 – 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

#### F.9.11 TLV Coding of Field 46 (CAD Management/Service Quality Data)

This field is TLV coded according to the definition in section F.9.1. Table F.105 on page F–97 gives the relation between messages and applicable tags.

Table F.94 – Applicable values for Field 46 (CAD Management/Service Quality Data)

Tag	Item	Attrib.	Length <sup>2)</sup>	Value
T2	PIN Pad ID	b8	12	IDPPCREATOR    IDPP
T3	MAD-Handler ID	ans8	12	See below
T4	Terminal Capabilities	b3	7	See ref. 36: "EMV, version 4.1"
T5	Additional Terminal Capabilities	b5	9	See ref. 36: "EMV, version 4.1"
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. 36: "EMV, version 4.1"
TB	Info Level	b1	5	
TC	Update Results	..b99	..103	Generated by the PSAM
TD	Response time for previous on-line transaction <sup>1)</sup>	b18	22	Coded as PSAM identifier (13 bytes), STAN (3 bytes) and response times in milliseconds (2 bytes)
TE	Number of time-outs <sup>1)</sup>	n2	5	For APACS messages, including advices and administrative messages
TF	Number of card reader errors <sup>1)</sup>	n2	5	Including magnetic stripe card errors
TG	Number of unsupported cards <sup>1)</sup>	n2	5	
TH	Number of communication errors between CAD and Merchant Application <sup>1)</sup>	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	b1	5	
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

**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.  
Example: Tag TF indicating 12 card reader errors: 54 46 00 01 12

- F.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 F.95.

Table F.95 – Coding of the MAD–Handler ID

Name	Attributes	Length	Remarks
Terminal Manufacturer Id.	ans3	3	Identifier assigned by PBS
Terminal Serial Number	ans5	5	Individual MAD–Handler Id.

### F.9.12 Coding of Field 47 (Additional Data – National)

This field is TLV coded according to the definition in section F.9.1.

Table F.96 – Applicable values for Field 47 (Additional Data – National)

Tag	Item	Attrib.	Value
TL	KEK <sub>PIN</sub> Version	b1	
TM	[KSES <sub>PIN</sub> ]	b16	
TN	PIN Block Format	n1	Allowed values are 0, 1 and 2
V5	CV–2	an3	Card verification data (for key entered transactions)
TX	Issuer Envelope Data	..b150 <sup>1)</sup>	To be provided by the terminal using the <i>Set Debit/Credit Properties</i> command
<b>Legend:</b>			
<sup>1)</sup> = Maximum value for EMV transactions is limited to 60 bytes.			

### F.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. 36: “EMV, version 4.1”.

**NOTE:** This coding is different from the TLV coding defined for other fields in section F.9.1.

Table F.97 – Field 55 for Request and Advice Messages

Name	Tag	Attributes	Length <sup>1)</sup>	Remarks	
Application Cryptogram	M	'9F26'	b8	11	ARQC/TC/AAC
Cryptogram Information Data	M	'9F27'	b1	4	
Issuer Application Data	C <sup>2)</sup>	'9F10'	..b32	..35	
Unpredictable Number	C <sup>3)</sup>	'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 <sup>4)</sup>	'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
Authorisation Response Code	C <sup>5)</sup>	'8A'	an2	4	For cryptogram verification
Transaction Currency Code	M	'5F2A'	n3	5	Also present in field 49
Issuer Script Results	C <sup>6)</sup>	'D0'	b5	7	PBS-defined Tag
Maximum number of bytes				136	
<b>Legend:</b>					
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. The number of Issuer Script Results depends on the number of Issuer scripts delivered in the previous host response!					



Table F.98 – Field 55 for Response Messages

Name	Tag	Attributes	Length <sup>1)</sup>	Remarks
Issuer Authentication Data	O	'91'	b8..b16	10..18
Issuer Script 1	O	'71'	..b127	..129
Issuer Script 2	O	'72'	..b127	..129
<b>Legend:</b>				
O: Optional				
1) Length includes the total length of Tag, length and Value.				

**NOTE:** The data elements listed in table F.98 may be absent.

#### F.9.14 Coding of Field 56 (Original Data Elements)

This field uniquely identifies a previously performed Authorization Request, Financial Request or Financial Advice.

Table F.99 – 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 <sub>PSAM</sub>	b5	5	The entity assigning PSAM Creator Ids
ID <sub>PSAMCREATOR</sub>	b4	4	The entity assigning PSAM Ids
ID <sub>PSAM</sub>	b4	4	Individual PSAM Id

#### F.9.15 Coding of Field 60 (PSAM Identifier)

This field uniquely identifies a given PSAM.

- F.9.15.1 A Field 60 (PSAM Identifier) shall be coded according to table F.100.

Table F.100 – Field 60 (PSAM Identifier)

Name	Attributes	Length	Remarks
RID <sub>PSAM</sub>	b5	5	The entity assigning PSAM Creator Ids
ID <sub>PSAMCREATOR</sub>	b4	4	The entity assigning PSAM Ids
ID <sub>PSAM</sub>	b4	4	Individual PSAM Id

- F.9.15.2 A As Field 60 is an LVAR field, the PSAM Identifier shall be preceded by a one-byte length field with the value '0D'.

### F.9.16 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'.

### F.9.17 Coding of Field 62 (Merchant Initiative)

This field contain flags indicating whether the CVM and/or on-line/offline is forced by the merchant.

F.9.17.1 A Field 62 (Merchant Initiative) shall be coded on one byte according to table 9.6.

F.9.17.2 A As Field 62 is an LVAR field, the Merchant Initiative shall be preceded by a one-byte length field with the value '01'.

### F.9.18 TLV Coding of Field 63 (PSAM Updates)

This field is TLV coded according to the definition in section F.9.1.

F.9.18.1 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 6.16.7.

Table F.101 – Applicable values for Field 63 (PSAM Updates)

Tag	Item	Attrib.	Value
TO	PSAM Update	b..MAX	C-APDU to send to the PSAM

F.9.18.2 A As Field 63 is an LLVAR field, the PSAM Updates shall be preceded by a two-bytes length field.

### F.9.19 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.

## **F.9.20 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 F.102)
- Airlines/Passenger Transport (see table F.103)
- Car Rental/Vehicle Rental (see table F.104)

This page is intentionally left blank

Table F.102 – 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.	<b>Mandatory.</b> 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 <b>Mandatory.</b>
H3	Departure date	n8	The day the cardholder checked out.	YYYYMMDD <b>Mandatory.</b>
H4	Folio number	an10	The number assigned to the lodging message.	<b>Mandatory.</b>
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.
HT	Total tax	n12	Total tax amount.	Same currency as 1240 presentment, field 49.

Tag	Item	Attrib.	Description	Value
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. <b>Mandatory.</b>
HX	Tot-records	n4	Total lodging addendums associated with same presentment.	Max. 99. <b>Mandatory.</b>

Table F.103 – 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.	<b>Mandatory.</b>
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.	<b>Mandatory.</b>
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.	<b>Mandatory.</b>
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. <b>Mandatory.</b>
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. <b>Mandatory.</b>
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.



Tag	Item	Attrib.	Description	Value
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 <b>Mandatory.</b>
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.
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)

Tag	Item	Attrib.	Description	Value
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.	
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 <b>Mandatory.</b>
HX	Tot-records	n4	Total passenger addendum records associated with the same presentment.	Max. 99 <b>Mandatory.</b>

Table F.104 – 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.	<b>Mandatory.</b>
I1	Person name	an40	Name of person renting the vehicle.	<b>Mandatory.</b>
I2	Rental return city	an25	Name of city where vehicle was returned.	<b>Mandatory.</b>
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.	<b>Mandatory.</b>
H6	Service phone number	an12	Customer support number that can be used by the cardholder.	<b>Mandatory.</b>
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.	
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.	

Tag	Item	Attrib.	Description	Value
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.
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 <b>Mandatory.</b>
HX	Tot-records	n4	Total vehicle rental addendums associated with the same presentment.	Max. 99 <b>Mandatory.</b>

Table F.105 – 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	
		Item/MTI	0106	0116	0126	0136	0206	0216	0226	0236	0360	0370	0426	0436	0624	0634	0624
T2	PIN Pad ID	C <sup>1)</sup>		O		C <sup>1)</sup>											
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, C<sup>1)</sup> = if CVM = PIN

Table F.105 – 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											

# Attachment G. Receipts

## G.1 Receipts

All lay-outs shown in this section are based on a receipt printer able to print 24 characters per line.

Examples showing the layout of receipts for printers with 18 characters per line are also included.

### G.1.1 General Requirements

The general requirement for printing receipts defines that the cardholder shall be able to get a receipt when the cardholder has accepted the payment.

How and when the cardholder accepts the payment depends on the CVM selected.

This section defines how the general requirement is translated into a number of specific requirements.

G.1.1.1 A A cardholder receipt shall as minimum be printed in the following cases, provided that the *Initiate Payment* command has been issued:

- The transaction is successful,
- A receipt to be signed by the cardholder has been printed,
- The cardholder has pressed the Accept button,
- The MAD-Handler is not aware whether the cardholder has pressed the Accept button or not.

**NOTE:** Information on cardholder actions from the User Interface Handler to the MAD-Handler is optional and may be implemented by use of proprietary means.

G.1.1.2 A Requirement G.1.1.1 does not apply if one of the following conditions are met:

- The cardholder has chosen not to have a receipt.
- The ASW1-ASW2 returned in the response to *Initiate Payment* command has the value '1222' or '1400'.

G.1.1.3 A If signature forms part of the CVM selected, the receipt to be signed by the cardholder shall be printed after the response to *Validate Data* command is known, but before the *Complete Payment* command is issued to the PSAM.

The result from signature validation shall be included in the *Complete Payment* command. In this way, the merchant can stop/cancel the transaction. 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.

- G.1.1.4 A 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.

**NOTE:** Requirement G.1.1.4 does not apply if signature forms part of the CVM selected if the receipts are printed on dual-layer paper with carbon copy. Requirements for this case are defined in section G.2.9.

- G.1.1.5 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.

### **Special Considerations for Unattended Terminals**

- G.1.1.6 A For a unattended terminal, the cardholder shall be asked to select whether or not a receipt is wanted.

- G.1.1.7 B The default shall be *not* to print a receipt for an unattended terminal.

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. petrol stations, the transaction processing is split into four steps :

- Pre-authorization using the physical card and a default 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.

Single-user terminals shall fulfil requirement G.1.1.8, whereas multi-user terminals shall fulfil requirements G.1.1.9 to G.1.1.11.

- G.1.1.8 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.

- G.1.1.9 A If access to the user interface is shared with other cardholders throughout the entire transaction, the decision whether a receipt shall be printed or not shall be taken via cardholder dialogue during the pre-authorization part of the transaction.

- G.1.1.10 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.

**NOTE:** The method for selecting receipt printing depends on the environment. In petrol stations, the pump number could be used to select the cardholder's receipt.

**NOTE:** Reading the card again after delivery of service is not a feasible way to identify a specific receipt, due to card technology.



G.1.1.11 A No receipt shall be printed unless the cardholder chose receipt printing during the pre–authorization part of the transaction.

G.1.1.12 A 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.

## G.1.2 General Layout for Receipts

Figure G.1 gives an overview of general layout for receipts. The lines present in a receipt depends on the actual Business Call. Requirements to individual lines are defined succeeding.

The general receipt layout defined in this section only specifies the layout when a transaction is completed successfully.

Variation in the layout if the transaction has failed or has been rejected are defined in succeeding sections.

Line	Receipt	Purchase/ Refund	Original Auth. (PIN only)	Gratuity (signature only)	Capture
	Specification of service, slogan, clerk etc.	O	O	O	O
1	PBS – TESTSHOP	M	M	M	M
2	LAUTRUPBJERG 10	M	M	M	M
3	2750 BALLERUP	M	M	M	M
4	TLF. 44 68 44 68	O	O	O	O
5	CVR.NR. 12345678	O	O	O	O
6		M	M	M	M
7	2000-06-24 18:15	M	M	M	M
8		M	M	M	M
9	KØB DKK 123456,78	M	M	M	M
10	EKSTRA DKK	–	–	M	–
11		–	–	M	–
12	TOTAL DKK	–	–	M	–
13		M	M	M	M
14	DANKORT PSN: 01	M	M	M	M
15	XXXX XXXX XXXX XXX6 789	M	M	M	M
16	TERM: 1F2G3H4I-123456	M	M	M	M
17	I@1 PBS NR:1234567890	M	M	M	M
18		–	–	M	–
19	** VED EKSTRA **	–	–	M	–
20	HUSK NY KVITTERING	–	–	M	–
21	** WHEN TIPPING **	–	–	M	–
22	ASK FOR NEW RECEIPT	–	–	M	–
23		C1	–	M	C2
24	KORTHOLDERS SIGNATUR:	C1	–	M	C2
25		C1	–	M	C2
26		C1	–	M	C2
27		C1	–	M	C2
28	.....	C1	–	M	C2
29		M	M	M	M
30	ATC:12345 AED:000124	C3	C3	C3	C3
31	AID: 0123456789ABCDEF	C3	C3	C3	C3
32	PSAM: 1234567-1234567890	M	M	M	M
33	ARC:AB STATUS:1234	C4	C4	C4	C4
34	AUT KODE: 1A2B3C	C5	C5	C5	C5
35	REF:123456 AUTORISERET	M	–	M	M
36		M	M	M	M
	Specification of service, slogan, clerk etc.	O	O	O	O

**Legend:**  
– = not applicable, M = Mandatory, O = Optional, C= Conditional where:  
C1 = Signature based transactions.  
C2 = Signature based transaction with no gratuity.  
C3 = EMV based transaction.  
C4 = ARC only present if EMV based transaction.  
C5 = If Approval Code is present.

Figure G.1 – Receipt overview

- G.1.2.1 B Line 1. The data element “ME<sub>NAME</sub>” shall be printed.
- G.1.2.2 B Line 2. The data element “ME<sub>ADDRESS</sub>” shall be printed.
- G.1.2.3 B Line 3. The data elements “ME<sub>ZIP</sub>” and “ME<sub>CITY</sub>” shall be printed.
- G.1.2.4 C Line 4. The data element “ME<sub>PHONE</sub>” or additional information may be printed.
- G.1.2.5 C Line 5. Additional information identifying the merchant (e.g. ME<sub>BRN</sub>) may be printed.
- G.1.2.6 C If no data is printed in line 4 and 5, the respective lines may be omitted.
- G.1.2.7 A Line 6. If the printed receipt is a copy of the previous receipt, line 6 shall be expanded to 5 lines as shown in figure M.1.



Figure G.2 – Receipt – copy

- G.1.2.8 A Line 7. The date and time shall be printed in the format:  
YYYY–MM–DD hh:mm  
**NOTE:** Seconds may be indicated using the format:  
YYYY–MM–DD hh:mm:ss
- G.1.2.9 A If the printed receipt is a copy, date and time shall be the same as the date and time printed on the original receipt.
- G.1.2.10 A Line 8. The line shall be blank.
- G.1.2.11 A Line 9. The text (“KØB” in the example) shall be according to table G.1.

Table G.1 – Business Call and related print text

Business Call, etc.	Print text
Purchase, Gratuity and Capture	KØB
Refund	RETUR
Original Authorization	BELØB

- G.1.2.12 A Line 9. The Alphabetic Currency Code (e.g. “DKK”) shall be generated based on the data element “CURRC”.

- G.1.2.13 A Line 9. The amount shall be printed according to table G.2.

Table G.2 – Business Call and related amounts to be printed

<b>Business Call, etc.</b>	<b>Amount printed</b>
Purchase, Refund and Capture	<b>Amount, transaction.</b> The Amount is the final amount, i.e. the amount that will be transferred to the Merchant's account.
Original Authorization	<b>Amount, transaction.</b> The amount authorized. If the amount is not relevant to the cardholder, the amount shall be omitted.
Gratuity	Amount for goods and services before gratuity is added.

- G.1.2.14 A Line 10. The text “EKSTRA” shall be fixed. The Alphabetic Currency Code (e.g. “DKK”) shall be generated based on the data element “CURRC”.

- G.1.2.15 A Line 11. The amounts in line 9 and 10 shall be underlined.

- G.1.2.16 A Line 12. The text “TOTAL” shall be fixed. The Alphabetic Currency Code (e.g. “DKK”) shall be generated based on the data element “CURRC”.

- G.1.2.17 A Line 13. The amount in line 9 (or 12) shall be underlined.

- G.1.2.18 A Line 14. The data element “Card Name” shall be printed.

**NOTE:** The actual contents of Card Name is specified in requirements 6.10.6.11 (EMV), 6.12.6.12 (MSC), 6.13.6.13 (Key Entered).

- G.1.2.19 A Line 14. The text “PSN:” shall be fixed. The data element “PANSEQUENCE” shall be printed as two decimal digits.

**NOTE:** As the data element “PANSEQUENCE” is optional in the EMV card, the text “PSN:” and succeeding data should be omitted if the value returned in the *Initiate EMV Payment* or *Initiate Token Based Payment* response is not in a valid format (BCD) or not included.

- G.1.2.20 A Line 15. The data element “PAN” shall be truncated according to section G.3.1 when printed.

- G.1.2.21 A Line 15. The printed value of the PAN shall be left justified and divided in blocks of 4 digits (the last block may consist of 1, 2, 3 or 4 digits).

- G.1.2.22 A Line 16. The text “TERM:” shall be fixed. The data element “Terminal Identification” shall be printed as 8 alphanumeric characters.

- G.1.2.23 A Line 16. The data element “STAN” shall be printed as 6 digits with leading zeroes.
- G.1.2.24 A Line 17. The conditions for the transaction shall be indicated by three character code (“I@1” in the example). See section G.3.2 for coding.
- G.1.2.25 A Line 17. The text “PBS NR:” shall be fixed and the data element “ME<sub>NUMBER</sub>.” shall be printed as 10 digits with leading zeroes.
- G.1.2.26 A Line 18. The line shall be blank.
- G.1.2.27 A Line 24. For Refund transactions the text shall be changed to indicate that the receipt shall be signed by the merchant. See figure G.3.

FORRETNINGENS SIGNATUR:	24ref
-------------------------	-------

Figure G.3 – Receipt – Refund

- G.1.2.28 A Line 23 – 28. These lines contains fixed text. Conditions for printing of these lines are defined in figure G.1.
- G.1.2.29 A Line 29. This line shall be blank.
- G.1.2.30 A Line 30. The text “ATC:” (Applications Transaction Counter) shall be fixed. The data element “ATC” shall be printed as five decimal digits with leading zeroes.
- G.1.2.31 A Line 30. The text “AED:” (Applications Effective Date) shall be fixed. The data element “Applications Effective Date” shall be printed as six digits indicating YYMMDD.

**NOTE:** As the data element “Application Effective Date” is optional in the EMV card, the text “AED” and succeeding date should be omitted if the value ‘000000’ is returned in the *Initiate EMV Payment* response.

- G.1.2.32 A Line 31. The text “AID:” (Application Identifier) shall be fixed. The data element “AID” shall be printed as up to 32 hexadecimal characters.

**NOTE:** If the AID exceeds 20 hexadecimal characters, the AID may be split in two lines, where the first ten hexadecimal characters shall be included in the the first line.

AID:	A000000001	31a
.....	—123456789ABCDEF	31b

Figure G.4 – Receipt – example of line 31

- G.1.2.33 A Line 30 – 31. Conditions for printing of these line shall be according to figure G.1.

- G.1.2.34 A Line 32. The text “PSAM:” shall be fixed. The seven least significant decimal digits of the data element “ID<sub>PSAM</sub>CREATOR” concatenated with the data element “ID<sub>PSAM</sub>” shall be printed as 7 + 10 digits.
- G.1.2.35 A Line 33. The text “ARC:” (Authorisation Response Code) shall be fixed. The data element “Authorisation Response Code” shall be printed as two alphanumeric characters.
- NOTE:** The value to be printed as Authorization Response Code shall be fetched from the *Validate Data 2* response.
- NOTE:** As the data element Authorization Response Code is only relevant for EMV transactions, the text “ARC:” and succeeding value shall be omitted if the value ‘0000’ is returned in the *Validate Data 2* response.
- NOTE:** If the baseline message format for *Validate Data* command and response has been used, the data element Authorisation Response Code shall be fetched from field 44 in the host response.
- G.1.2.36 A Line 33. The text “STATUS:” shall be fixed. The data element “Action Code” shall be printed as four digits.
- NOTE:** The value to be printed as Action Code shall be fetched from the data element Action Code<sub>PRINT</sub> in the *Validate Data 2* response.
- NOTE:** If the baseline message format for *Validate Data* command and response has been used, the The data element ”Action Code” shall be fetched from field 39 in the host response. In case of an offline transaction, the text may be omitted.
- G.1.2.37 A Line 33. Conditions for printing of this line shall be according to figure G.1.
- G.1.2.38 A Line 34. The text “AUT KODE:” (Approval Code) shall be fixed. The data element “Approval Code” shall be printed as six alphanumeric characters.
- NOTE:** The data element Approval Code shall be fetched from the *Validate Data 2* response.
- NOTE:** If the baseline message format for *Validate Data* command and response has been used, the data element Approval Code shall be fetched from:
- field 38 in the host response (if a host response is available)
  - the response to *Check Stop List* command (if the value has been manually entered by the merchant).

- G.1.2.39 A Line 34. Conditions for printing of this line shall be according to figure G.1.
- G.1.2.40 A Line 35. The text “REF:” (Reference no. for cardholder’s account statement) shall be fixed. The data element “STAN” shall be printed as six digits.
- G.1.2.41 A Line 35. The text “AUTORISERET” shall only be printed if the transaction is completed successfully.
- G.1.2.42 C Line 35. The text “AUTORISERET” may be substituted by ”GENNEMFØRT” if the following conditions are both fulfilled:
- the transaction is completed successfully,
  - a Financial Request (MTI 0206 or 0207) has been exchanged successfully as part of the transaction, i.e. all messages with financial impact have been transferred successfully.
- G.1.2.43 A Line 36. This line shall be blank.

## G.2 Receipt Variants

### G.2.1 General Requirements

In section ‘G.1.2 General Layout for Receipts’ the requirements for the layout and the contents of the receipts are defined, but only if the transaction is completed successfully and if the terminal is installed in a non–banking environment.

In the present section additional requirements depending on transaction result, terminal implementation, environment etc. are defined.

These requirements are divided according to the following criteria:

- Receipts for Declined Transactions
- Receipts for Failed Transactions
- Receipts for Rejected Signature
- Original Authorization
- Reversal (Authorization)
- Transaction Stopped/Cancelled
- Reversal due to technical problems
- Receipts without Carbon Copy (single–layer paper)
- Receipts with Carbon Copy (dual–layer paper)
- Information concerning Euro currency
- Information concerning fees
- Manual Cash Disbursement

The transaction result is determined from the Application Status Words (ASW1–ASW2) received in responses from the PSAM.

The value of ASW1–ASW2 may be used as guideline to determine whether the transaction was Declined, Failed or Stopped/Cancelled.

If more than one response from the PSAM indicates a non-approved result, the first such ASW1–ASW2 received is used for the receipt.

The following table shows how the transaction result may be determined from the resulting ASW1–ASW2 value (see also table 8.106 and 8.107):

Table G.3 – Guidelines for evaluating 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

- G.2.1.1 A Whenever a receipt shall be printed, including lines containing information not available at the time the receipt is printed, the default character(s) to print shall be 'space(s)'.

**NOTE:** Figure G.5 explains at which step during the transaction flow data elements are available.



Line	Receipt	Data Element	Presence						
1	PBS – TESTSHOP	ME <sub>NAME</sub>	A						
2	LAUTRUPBJERG 10	ME <sub>ADDRESS</sub>	A						
3	2750 BALLERUP	ME <sub>ZIP + ME<sub>CITY</sub></sub>	A						
4	TLF. 44 68 44 68	ME <sub>PHONE</sub>	A						
5	CVR.NR. 12345678	ME <sub>BRN</sub>	A						
6									
7	2000–06–24 18:15	DTHR	A						
8									
9	KØB DKK 123456,78		O	O					
10	EKSTRA DKK		O	O					
11									
12	TOTAL DKK	Amount	A1	B					
13									
14	DANKORT PSN: 01	Cardname		B					
		PAN <sub>SEQUENCE</sub>		B					
15	XXXX XXXX XXXX XXX6 789	PAN		B					
16	TERM: 1F2G3H4I–123456	Terminal Identification	A						
		STAN		B			E1	F1	
17	I@1 PBS NR:1234567890	Transaction Condition Code			C			F2	
		ME <sub>NUMBER</sub>	A						
...									
29									
30	ATC:12345 AED:000124	Application Transaction Counter			C				
		Application Effective Date		B					
31	AID: 0123456789ABCDEF	Application Identifier	A						
32	PSAM: 1234567–1234567890	ID <sub>PSAMCREATOR</sub> + ID <sub>PSAM</sub>	A						
33	ARC:AB STATUS:1234	Authorization Response Code				D		F	
		Action Code				D		F	
34	AUT KODE: 1A2B3C	Approval Code				D		F	
35	REF:123456 AUTORISERET	STAN		B			E1	F1	
		"Transaction Result"							G
36									

**Legend:**  
**O** = Optional.  
**A:** Data elements to be present before the *Initiate Payment* command is issued  
A1: If amount has been entered/approved  
**B:** Data elements to be added after successful response to the *Initiate Payment* command  
**C:** Data elements to be added after successful response to the *Payment* command  
**D:** Data elements to be added after host response (Baseline – no Service Packs supported)  
**E:** Data elements to be added after the *Validate Data* response (Baseline – no Service Packs supported)  
E1: In case of PIN retry  
**F:** Data elements to be added after the *Validate Data* response (Service Packs supported)  
F1: In case of PIN retry  
F2: Replaces previous value  
**G:** Data elements to be added after the *Complete Payment* response

Figure G.5 – Presence of Data Elements

- G.2.1.2 B If a transaction is not completed successfully and a receipt is printed, the Application Status Words (ASW1–ASW2), indicating the reason for the unsuccessful result, shall be printed at the bottom of the receipt.

**NOTE:** The value for ASW1–ASW2 shall be printed as 4 hexadecimal characters as shown in figure G.6.

ASW1-ASW2: ABCD
-----------------

Figure G.6 – ASW1-ASW2 value printed on receipts

### G.2.2 Receipt for Declined Transaction

A transaction may be 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). This section defines the requirements if a transaction is declined and the receipt shall be printed.

*****	36afv1
AFVIST	36afv2
*****	36afv3
< ERROR MESSAGE >	36afv4

Figure G.7 – Receipt – Declined

- G.2.2.1 A Lines 18 – 28 and 34 – 35 shall be omitted.
- G.2.2.2 A Line 36. This line shall be expanded according to figure G.7, lines 36afv1 –36afv3 to include a message saying that the transaction was declined:
  - 36afv1 and 36afv3: These lines shall be filled with either ‘\*’ or ‘#’ characters.
  - 36afv2: The text “AFVIST” shall be fixed.
- G.2.2.3 C Line 36. If the terminal is able to generate a short textual message explaining the reason for the decline, this message may be printed according to figure G.7, line 36afv4.

### G.2.3 Receipt for Failed Transaction

A transaction may fail, 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). This section defines the requirements if a transaction has failed and a receipt shall be printed.

*****	36afb1
AFBRUDT – FEJL	36afb2
*****	36afb3
	36afb4

Figure G.8 – Receipt – Failed

- G.2.3.1 A Line 36. This line shall be expanded according to figure G.8 to include a message saying that the transaction failed:

36afb1 and 36afb3: These lines shall be filled with either ‘\*’ or ‘#’ characters.  
 36afb2: The text “AFBRUDT – FEJL” shall be fixed.

- G.2.3.2 A Line 18 – 31 and 34 – 35 shall be omitted.
- G.2.3.3 C In line 33, the data element “Action Code” may be printed as four space characters.
- G.2.3.4 C If the terminal is able to generate a short textual message explaining details about the failure, this message may be printed in line 36afb4.

**NOTE:** A textual message may e.g. indicate that a communication failure has occurred, by referring to the relevant Connection Error counter.

### G.2.4 Receipt for Rejected Signature

Verification of the cardholder signature written on the receipt may require action from the merchant. This section defines the requirements if the signature is not accepted.

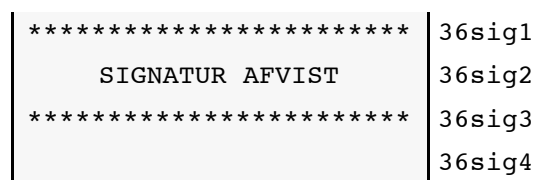


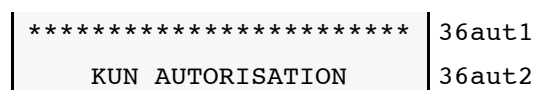
Figure G.9 – Receipt – Signature Rejected

- G.2.4.1 A If the signature was not accepted by the Attendant, the cardholder’s receipt shall indicate that the signature was rejected.
- G.2.4.2 A Line 18 – 28 and 35 shall be omitted.
- G.2.4.3 A Line 36. The line shall be expanded according to figure G.9 to include a message saying that the signature was not accepted:

36sig1 and 36sig3: These lines shall be filled with either ‘\*’ or ‘#’ characters.  
 36sig2: The text “SIGNATUR AFVIST” shall be fixed.

### G.2.5 Original Authorization

If the cardholder has accepted an Original Authorization by entering the PIN, the receipt printed shall indicate that an authorization only has been completed.



*****	36aut3
	36aut4

Figure G.10 – Receipt – Original Authorization

G.2.5.1 A Line 36. The line shall be expanded according to figure G.10 to include a message saying that the signature was not accepted:

36aut1 and 36aut3: These lines shall be filled with either ‘\*’ or ‘#’ characters.  
 36aut2: The text “KUN AUTORISATION” shall be fixed.

### Unattended Terminals

G.2.5.2 B If the amount authorized is not relevant to the cardholder, the amount shall be omitted on the receipt, i.e. space characters shall be printed in line 9 instead of the amount value.

**NOTE:** In some environments, e.g. self service petrol terminals, the amount authorized have no importance and may even be confusing to the cardholder.

If the exact amount is not know at the time of authorization e.g. self service petrol terminals, the Business Call Original Authorization may be used to initiate a payment sequence.

Even if the exact amount is know at the time of authorization, the Business Call Original Authorization may be used to initiate a payment sequence. In this case the amount is shown to the cardholder for acceptance during the Original Authorization. If the delivery of the selected goods is awaiting the result of the Original Authorization, the Capture may be initiated after a successful delivery of goods. This procedure may be relevant for e.g. ticket vending machines.

If an Original Authorization is rejected/failed in such an unattended environment, the printing of the resulting receipt(s) should be controlled according to the following requirements.

G.2.5.3 B If

- the terminal is unattended, and
- the payment sequence is Token based, and
- the transaction sequence is interrupted/cancelled before the Capture is completed,

printout of receipt(s) shall include a receipt for all the Original Authorizations performed, i.e. both for rejected, failed and approved authorization attempts.

G.2.5.4 B If

- the terminal is unattended, and
- the transaction sequence is Token based, and
- the amount is *not* shown to the cardholder, and

- the Capture is completed before printout of receipt is requested/initiated,
- only the receipt(s) derived from the Capture(s) shall be printed.

G.2.5.5 B If

- the terminal is unattended, and
- the transaction sequence is Token based, and
- the amount is shown to the cardholder, and
- the Capture is completed before printout of receipt is requested/initiated,

printout of receipt(s) shall include a receipt for all the non successful Original Authorizations performed and the final Capture.

## G.2.6 Reversal (Authorization)

If an Original Authorization (and possibly one or more subsequent Supplementary Authorizations) has been completed successfully, a Token will be available.

If the payment process is going to be completed by other means than the card data available in the Token, the Token should be ‘released’ by initiating the Business Call Reversal (Authorization).

When a Token is ‘released’ the cardholder may request a receipt as documentation for the authorization being voided.

The additional receipt shall contain information according to the following requirements.

G.2.6.1 A Line 6. This line shall be expanded to 5 lines as shown in figure G.11.

	6rev1
*****	6rev2
ANNULLERING (AUT)	6rev3
*****	6rev4
	6rev5

Figure G.11 – Receipt – Reversal (Line 6)

- 6rev2 and 6rev4: These lines shall be filled with either ‘\*’ or ‘#’ characters.
- 6rev3: The text ”ANNULLERING (AUT.)” shall be fixed.

G.2.6.2 A Line 18 – 28 shall be omitted.

G.2.6.3 A Line 36. The line shall be expanded according to figure G.12 to include a message saying that the authorization has been voided:

*****	36rev1
ANNULLERING (AUT.)	36rev2
*****	36rev3
	36rev4

Figure G.12 – Receipt – Reversal (Line 36)

- 36rev1 and 36rev3: These lines shall be filled with either ‘\*’ or ‘#’ characters.
- 36rev2: The text ”ANNULLERING (AUT.)” shall be fixed.

**Unattended Terminals**

G.2.6.4 B If the amount authorized is not relevant to the cardholder, the amount shall be omitted on the receipt, i.e. space characters shall be printed in line 9 instead of the amount value.

**NOTE:** In some environments, e.g. self service petrol terminals, the amount authorized have no importance and may even be confusing to the cardholder.

G.2.6.5 B If

- the terminal is unattended, and
- the payment sequence is Token based, and
- the transaction sequence is interrupted/cancelled before the Capture is completed,

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.

**G.2.7 Transaction Stopped/Canceled**

The attendant may stop a transaction in process by pressing a cancel key.

*****	36can1
AFBRUDT – CANCEL	36can2
*****	36can3
	36can4

Figure G.13 – Receipt – Transaction Stopped by Attendant

G.2.7.1 C If the merchant or the cardholder stops a transaction in progress before the cardholder has accepted the transaction by entering the PIN, a receipt may be printed where lines 18 – 36 are omitted and line 36 expanded according to figure G.13.

- 36can1 and 36can3: These lines shall be filled with either ‘\*’ or ‘#’ characters.

36can2: The text “AFBRUDT – CANCEL” shall be fixed.

- G.2.7.2 A If the merchant or cardholder is able to stop a transaction in progress after the cardholder accepted the transaction by entering the PIN, a receipt shall be printed where lines 18 – 35 are omitted and line 36 expanded according to figure G.13.

## G.2.8 Receipts without Carbon Copy with Signature as CVM

In case of signature used as CVM, both the merchant and the cardholder shall get a receipt.

The merchant receipt shall include the cardholder’s signature manually written. If the receipt uses “dual–layer paper” (with carbon copy), both receipts will be printed at the same time, and the information printed will be identical.

If the receipt printer uses “single–layer paper” (without carbon copy, e.g. thermo paper) the two receipts cannot be printed at the same time, and the information printed may differ.

This section defines the requirements for the combination “single–layer paper” is used as basis for the printed receipt and signature is used as CVM.

- G.2.8.1 A Both the merchant and the cardholder shall get a printed receipt for each transaction or function.

**NOTE:** The receipts may be printed as two subsequent and identical receipts.

- G.2.8.2 A If the paper used in the receipt printer does not include a carbon copy, two receipts shall be printed (one for the merchant and one for the cardholder).

The master receipt printed shall be signed by the cardholder (or the merchant for Refund transactions).

- G.2.8.3 A The second receipt printed (the copy) shall include the same data information and in the same format as the master.

- G.2.8.4 A The master and the copy receipts shall be identical, but the lines 23 – 28, holding the signature panel, shall be omitted on the copy.

- G.2.8.5 A The function for printing a copy of the previous receipt shall include printing of both the master and the copy receipts.

- G.2.8.6 A Two different messages shall be printed on the master and copy receipts as defined in requirement G.2.8.7 and G.2.8.8.

- G.2.8.7 A For all transactions/functions, except for Refund, line 36 shall be expanded according to figure G.14 and G.15 to include the messages:

	36for1
FORRETNINGENS NOTA	36for2

Figure G.14 – Master Receipt

	36kor1
KORTHOLDERS KOPI	36kor2

Figure G.15 – Copy Receipt

- G.2.8.8 A For Refund transaction line 36 shall be expanded according to figure G.16 and G.17 to include the messages:

	36kor1
KORTHOLDERS KOPI	36kor2

Figure G.16 – Master Receipt

	36for1
FORRETNINGENS NOTA	36for2

Figure G.17 – Copy Receipt

- G.2.8.9 C If the transaction/function did not complete successfully, the copy receipt may be omitted.

## G.2.9 Receipts with Carbon Copy and Signature as CVM

In case of signature used as CVM and the receipt is printed on dual-layer paper with carbon copy, the cardholder's signature will be indicated on both papers.

The merchant shall keep the original receipt on which the cardholder's signature is written with ink.

- G.2.9.1 A A text saying 'keep original, copy to cardholder' shall be printed on the receipts. If this text is not included as a pre-printed information, line 36 shall be expanded according to figure G.18.

	36not1
BEHOLD NOTAEN	36not2
KOPI TIL KORTHOLDER	36not3

Figure G.18 – Receipt – Carbon Copy

- G.2.9.2 A If a receipt to be signed by the cardholder is printed but the final transaction result is unsuccessful due to a rejection of the cardholder's signature and/or the PSAM rejecting the *Complete Payment* command, a new receipt shall be printed. The receipt to be printed shall either be "Receipt for Failed Transaction"



(see section G.2.3) or “Receipt for Rejected Signature” (see section G.2.4).

### G.2.10 Additional Information Concerning EURO Currency

If a fixed exchange rate is defined between the transaction currency and the EURO currency, the corresponding amount in EURO currency may be printed as additional information on the receipt.

				36eur1
	KUN	TIL	INFORMATION:	36eur2
	BELØB	=	EUR 123456,78	36eur3
	1 EUR	=	DKK 12,345678	36eur4
				36eur5

Figure G.19 – Receipt – EURO Currency

- G.2.10.1 C Line 36. This line may be expanded according to figure G.19 to include a message, for information purposes only, defining the corresponding amount in EURO currency.
- G.2.10.2 A Line 36. This line shall not be expanded as defined in requirement G.2.10.1 if the exchange rate between the transaction currency and the EURO currency is not fixed.

### G.2.11 Cashback, Additional Fees etc.

If the final transaction amount consists of:

- the amount covering goods and services
- plus one or more additional amounts

all of the different amounts involved may be printed on the receipt.

Additional amounts added may either be:

- an addition requested or agreed by the cardholder before the transaction is initiated (e.g. Cashback) or
- a fee surcharge by the merchant.

This section do not cover Gratuity (or similar amounts) added by the cardholder while signing the receipt. But a Gratuity amount (or similar cardholder decided amounts) verbally or electronically agreed before the transaction is initiated is covered.

Additional amounts may be divided into the following three groups:

- Cashback, i.e. an amount of money payed out in cash by the merchant to the cardholder.
- Extra, i.e. a cardholder decided addition to be payed to the merchant

- Fee, i.e. an merchant decided surcharge to be added.

- G.2.11.1 A If the data element “Amount, Other” has a value different to zero, then Cashback shall be printed on the receipt as shown in figure G.20.

KØB	DKK	123386,43	9
BYTTEPENGE	DKK	100,00	9byt1
		_____	9byt2
TOTAL	DKK	123486,43	9byt3

Figure G.20 – Receipt – Cashback

- G.2.11.2 B If one or more of the subsets added to constitute the final transaction amount appears on the receipt, line 9 on the receipt shall be expanded as shown in figure G.21.

KØB	DKK	123386,43	9
GEBYR	DKK	34,56	9add1
BYTTEPENGE	DKK	12,34	9add2
EKSTRA	DKK	23,45	9add3
		_____	9add4
TOTAL	DKK	123456,78	9add5

Figure G.21 – Receipt – Additional Subsets

**NOTE:** Line 9add1 shall show the value of a transaction fee surcharged by the merchant.

**NOTE:** Line 9add2 shall show the value for Cashback.

**NOTE:** Line 9add3 shall show the value of an extra addition requested by the cardholder, e.g. tipping.

- G.2.11.3 A If one of the lines 9add1, 9add2 and 9add3 appears on the receipt, all the lines holding values different to zero shall appear too.
- G.2.11.4 A The order in which the lines 9add1, 9add2 and 9add3 appears on the receipt may be random, but shall be printed in consecutive lines.
- G.2.11.5 B If the receipt printed does not include lines 10 to 12, the word ‘TOTAL’ shall be used in line 9add5 instead of the word ‘BELØB’ (Amount).
- G.2.11.6 C If the receipt paper used makes it possible to print the complete word for Cashback ‘BYTTEPENGE’, the entire word may be printed instead.

## **G.2.12 Manual Cash Disbursement**

The terminal may in certain business environments be used for manual cash disbursement.

If the terminal is used for manual cash disbursement the receipt printed shall comply with the requirements defined in this section.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24                      18:15	7
	8c1
*****CASH*****	8c2
	8c3
CASH                      DKK    123456,78	9c
	13
MASTERCARD                      PSN: 01	14
XXXX XXXX XXXX XXX6 789	15
TERM:                      1F2G3H4I-123456	16
I@1                      PBS NR:1234567890	17
	18c1
PRINTED DIGITS:                      ....	18c2
IDENTIFICATION:	18c3
(PASSPORT ETC.)	18c4
	18c5
	18c6
.....	18c7
	18c8
CLERK ID:                      ....	18c9
	18c10
A FEE OR SET-UP CHARGE	19c
MAY BE ADDED TO THE	20c
CARDHOLDERS ACCOUNT	21c
BY THE CARD ISSUER	22c
	23
CARDHOLDERS SIGNATURE:	24c
	25
	26
	27
.....	28
	29
ATC:12345                      AED:000124	30
AID:                      0123456789ABCDEF	31
PSAM: 1234567-1234567890	32
ARC:AB                      STATUS:1234	33
AUT KODE:                      1A2B3C	34
REF:123456                      AUTORISERET	35
	36

Figure G.22 – Receipt – Manual Cash Disbursement  
(Example)

- G.2.12.1    A    Line 8. This line shall be expanded to three lines as shown in figure G.22, lines 7c1 – 7c3.

- G.2.12.2 A Line 9. The text in this line shall be substituted as shown in figure G.22, lines 9c.
- G.2.12.3 A Line 18. If signature forms part of the CVM selected, this line shall be expanded to ten lines for as shown in figure G.22, lines 18c1 – 18c10.
- The receipt printed shall include free space which enables the clerk to enter the following data manually (e.g. handwritten)
- the 4 digit printed below the embossed account number ('PRINTED DIGITS').
  - type and serial number of the additional identification document, e.g. passport ('IDENTIFICATION').
  - the name or identification code for the clerk ('CLERK ID').
- NOTE:** Line 18 shall not be expanded for PIN based transactions.
- G.2.12.4 C Line 18c9 – 18c10. These lines may be omitted if the information is already part of the header or footer of the receipt.
- G.2.12.5 A Line 19 – 22. The text in these lines shall be substituted as shown in figure G.22, lines 19c – 22c.
- G.2.12.6 A Line 24. The text in this line shall be substituted as shown in figure G.22, line 24c.

## G.3 Printing of PAN and Transaction Condition Codes

### G.3.1 Truncation of the PAN

In order to minimize the risk of misuse of receipts the PAN shall be truncated when printed on receipts.

- G.3.1.1 A The PAN shall be truncated according to table G.4.
- G.3.1.2 A The character capital 'X' shall be printed as masking character.
- G.3.1.3 A Truncation shall be made for all cards.
- G.3.1.4 A Truncation shall be made on all receipts and receipt copies handed over to the cardholder.
- G.3.1.5 C Truncation may be made on receipts kept by the merchant, e.g. receipts signed by the cardholder.

Table G.4 – Truncation vs. Number of Digits in the PAN

Number of digits	PAN	Truncated PAN
7	1234 567	XXXX 567
8	1234 5678	XXXX 5678
9	1234 5678 9	XXXX X678 9
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

### G.3.2 Transaction Condition Codes

The Transaction Condition Codes consist of three characters indicating Card Data Entry, CVM and Authorization respectively, see table G.5.

Table G.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 <sup>1)</sup>
T	Key entered	B	Offline PIN	4	(Referral)
I	ICC	C	No CVM	5	Refund (online/offline) or forced offline for other Business Calls <sup>1)</sup>
		M	Mail order		
		P	Phone order		
		V	(Online PIN and signature based)		
		W	Offline PIN and signature based		

**Legend:**

<sup>1)</sup> Code '3' shall be used if the transaction is performed offline and the Merchant Initiative does not indicate forced offline (i.e. B'xx0xxxxx) Code '5' shall be used if the transaction is performed offline and the Merchant Initiative indicates forced offline (i.e. B'x11xxxxx).

The code indicating Card Data Entry may 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:

- The actual sales site
- CVM Status

The code indicating Authorization may be based upon the following data:

- CVM Status (from *Validate Data 2* response)
- Business Call
- Merchant Initiative

## G.4 Additional Receipts for logging Purposes

### G.4.1 Introduction

A stand-alone terminal, i.e. a terminal with no interface to an electronic cash register system (or a similar payment system) may generate offline transactions without leaving any traces outside the terminal.

If such a terminal becomes defective while messages with financial impact are stored in the terminals Data Store, and none of these data can be read out or recreated, the financial consequences may be impossible to clear up in details.

If the terminal is interfaced to a cash register system or similar, a trace, a transaction log or even a complete Advice Log is expected to be stored in this system, and therefore outside the terminal.

In case the terminal becomes defective, the merchant will have full access to the log(s) stored outside the terminal.

If a transaction has been online approved, and the final amount is equal to the amount authorized, the host systems may be able to identify data elements not directly available from the terminal, if the terminal becomes defective.

If the merchant has kept a copy of the receipt, e.g. in case of a signature based transaction, this receipt may show all the relevant data, given that the all digits in the PAN are printed in clear text format.

If all the following conditions are fulfilled, a stand-alone terminal may printout a receipt copy for the merchant (e.g. in compressed format) to be kept together with the signature based receipts:

- The transaction is completed offline or the final transaction amount differs from the amount authorized,
- The transaction is not signature based, and therefore no receipt signed by the cardholder is stored,
- The terminal is not interfaced to an external cash register system in which the relevant transaction data is stored.

If a receipt copy (e.g. in compressed format) is printed for the merchant, this receipts shall contain the same transaction related data elements as the receipt handed over to the cardholder.

Figure G.1 defines the general layout for receipts handed over to the cardholder.

- G.4.1.1      B      With reference to this figure, a receipt copy should at least contain the data elements defined for the following lines in the general layout: 1, 7, 12, 14–17, 30–35, including the PAN in clear text.

#### **G.4.2    Signature based Transactions**

During signature based transactions an original receipt signed by the cardholder (and kept by the merchant) shall be printed together with a receipt copy for the cardholder.

If all the digits in the PAN are printed in clear text on the original receipt signed by the cardholder, the merchant will be able to store transaction information independently from the terminal.

#### **G.4.3    Refund Transactions**

During Refund transactions an original receipt shall be signed by the merchant and handed over to the cardholder.

A receipt copy for the merchant may be printed too.

If a receipt copy is printed for the merchant and all the digits in the PAN are printed in clear text on this receipt, the merchant will be able to store transaction information independently from the terminal.

The print out of a receipt copy for the merchant is relevant only for transactions accepted offline, i.e. when a Financial Advice message has been generated.

#### **G.4.4    PIN– and No–CVM based Transactions**

During PIN– and No–CVM based transactions a receipt shall be printed and handed over to the cardholder.

A receipt copy for the merchant has not been defined.

But if a receipt copy is printed for the merchant (e.g. in compressed format) and all the digits in the PAN are printed in clear text on this receipt, the merchant will be able to store transaction information independently from the terminal.

The print out of a receipt copy for the merchant is relevant only for transactions accepted offline, i.e. when a Financial Advice message has been generated.

The Business Call “Capture” completes successfully a Financial Advice message will be generated.



Even though the “Original Authorization” has been online approved, the “Capture” shall be considered as offline, since the amount may differ.

## **G.5 Receipts printed, depending on Business Environment and actual CVM**

This section defines guidelines concerning the printout of receipts depending on:

- the actual Business Environment (i.e. the merchant category and/or type of terminal),
- the Cardholder Verification Method (CVM) selected for the actual transaction and
- the actual step in the actual payment process (i.e. the actual Business Call).

The guidelines are built upon 5 different but representative Business Environments, as shown in the tables G.6.

Table G.6 – Receipts to be printed Vs. Business Environment

Business Environment (Examples)	Business Call	CVM			
		PIN	Signature	No CVM	Combined CVM
<b>Retail</b> Attended Terminal	Purchase	G.5.1	G.5.2	G.5.1	G.5.2
	Refund		G.5.3		
	Original Authorization				
	Supplementary Auth.				
	Capture				
	Reversal (Authorization)				
<b>CAT</b> Cardholder Activated Terminal (Self Service)	Purchase	G.5.1		G.5.1	
	Refund				
	Original Authorization				
	Supplementary Auth.				
	Capture	G.5.1		G.5.1	
	Reversal (Authorization)				
<b>Fuel Dispenser</b>  Self Service CAT	Purchase				
	Refund				
	Original Authorization				
	Supplementary Auth.				
	Capture	G.5.1		G.5.1	
	Reversal (Authorization)	G.5.7		G.5.7	
<b>Restaurant</b> Attended Terminal Supporting Gratuity/Extra	Purchase	G.5.8		G.5.8	
	Refund		G.5.3		
	Original Authorization		G.5.4		G.5.4
	Supplementary Auth.				
	Capture	G.5.1	G.5.5	G.5.1	G.5.5
	Reversal (Authorization)	G.5.7	G.5.7	G.5.7	G.5.7
<b>Hotel and Car Rental</b> Attended Terminal	Purchase				
	Refund		G.5.3		
	Original Authorization	G.5.6			G.5.6
	Supplementary Auth.				
	Capture	G.5.1	G.5.2	G.5.1	G.5.2
	Reversal (Authorization)	G.5.7	G.5.7	G.5.7	G.5.7
<b>Legend:</b> The letter/numbers indicates a reference to a subsection, later in this section, where the information concerning the actual receipts may be found. Grey cells indicates that the combination is not relevant. Empty cells indicates that printing of a receipt is not required					

Table G.7 – Business Environment – Characteristics

Business Environment	Characteristics
<b>General</b>	<ul style="list-style-type: none"> <li>• The total amount calculated by the merchant (or the merchants equipment) may include a fee surcharged by the merchant (and added to the total amount for goods and services).</li> <li>• The principles for calculating this type of extra payment is outside the scope of the present specification, and the calculation is considered to be completed when the total amount is known, i.e. when the transaction with financial impact is initiated (Purchase, Refund, Capture).</li> </ul>
<b>Retail</b> Attended Terminal	<ul style="list-style-type: none"> <li>• Terminals used in an attended environment, where the card payment is completed while the cardholder and the merchant is in a “face-to-face situation”.</li> <li>• The total transaction amount is (in principle) known before the card payment is initiated.</li> <li>• In case of PIN used as CVM, the total transaction amount is accepted by the cardholder during PIN entry.</li> </ul>
<b>CAT</b> Self Service	<ul style="list-style-type: none"> <li>• Self Service terminals used in an environment, where the total amount is known before the cardholder accepts the transaction, e.g. Ticket Vending Machines.</li> <li>• The total transaction amount is (in principle) known before the card payment is initiated.</li> <li>• In case of PIN used as CVM, the total transaction amount is accepted by the cardholder during PIN entry.</li> </ul>
<b>Fuel Dispenser</b> Self Service CAT	<ul style="list-style-type: none"> <li>• Self Service terminals used in an environment, where the total amount is not know when the cardholder accepts the payment process to be initiated, e.g. Fuel Dispensers.</li> <li>• The delivery of the “goods and services“ starts immediately after the cardholder’s acceptance.</li> <li>• The concluding Capture is generated immediately after the delivery of ‘goods and services’ is completed (i.e. within some minutes after the Original Authorization)</li> <li>• The Original Authorization is based on an estimated amount.</li> <li>• The total transaction amount indicated in the Capture should not exceed the amount authorized.</li> <li>• If the terminal is able to support several payment processes simultaneously, the print of receipts shall be initiated by the cardholder after Capture is completed. This function may require dedicated processing for identification of the receipt.</li> </ul>
<b>Restaurant</b> Supporting Gratuity/Extra	<ul style="list-style-type: none"> <li>• Terminals used in an attended environment, where the total transaction amount may not be known when the payment process is initiated.</li> <li>• The total transaction amount may not be known, since the cardholder may increase the transaction amount charged by the merchant, e.g. by adding Gratuity.</li> <li>• Only in case of Signature used as CVM (including Combined), addition of a cardholder decided extra amount may be possible unless it is added during the initial part of a Purchase.</li> <li>• The concluding Capture is generated immediately after the cardholder has accepted the transaction.</li> <li>• Supplementary Authorization may be required, depending on the actual card scheme, if the total transaction amount, incl. extra, exceeds the amount covered by the Original Authorization.</li> </ul>
<b>Hotel / Car Rental</b> Attended Terminal	<ul style="list-style-type: none"> <li>• Terminals used in an attended environment, where the concluding Capture may be postponed hours or days, compared to the Original Authorization.</li> <li>• Supplementary Authorizations may be required, if the final amount exceeds (or is expected to exceed) the amount already authorized.</li> </ul>

### G.5.1 PIN or No CVM

The receipt printed shall be based on the data received/generated during the Business Call:

- Purchase or
- Capture

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24	7
18:15	8
	9
KØB	10
DKK 123456,78	11
	12
	13
DANKORT	14
PSN: 01	15
XXXX XXXX XXXX XXX6 789	16
TERM: 1F2G3H4I-123456	17
### PBS NR:1234567890	18
	19
ATC:12345	20
AED:000124	21
AID: 0123456789ABCDEF	22
PSAM: 1234567-1234567890	23
ARC:AB	24
STATUS:1234	25
AUT KODE: 1A2B3C	26
REF:123456	27
AUTORISERET	28
	29
	30
	31
	32
	33
	34
	35
	36

Figure G.23 – Cardholder’s Receipt – PIN & No CVM

## G.5.2 Signature or Combined CVM (both PIN and Signature used)

The receipts printed shall be based on the data received/generated during the Business Call:

- Purchase or
- Capture

PBS – TESTSHOP	1		
LAUTRUPBJERG 10	2		
2750 BALLERUP	3		
TLF. 44 68 44 68	4		
CVR.NR. 12345678	5		
	6		
2000–06–24	18:15	7	
		8	
KØB	DKK	123456,78	9
		_____	13
DANKORT	PSN: 01		14
XXXX XXXX XXXX XXX6 789			15
TERM: 1F2G3H4I–123456			16
### PBS NR:1234567890			17
			23
KORTHOLDERS SIGNATUR:			24
			25
			26
			27
.....			28
			29
ATC:12345	AED:000124		30
AID: 0123456789ABCDEF			31
PSAM: 1234567–1234567890			32
ARC:AB	STATUS:1234		33
AUT KODE: 1A2B3C			34
REF:123456	AUTORISERET		35
			36.1
FORRETNINGENS NOTA			36.2

Figure G.24 – Signature or Combined CVM – Merchants Receipts

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24	7
18:15	8
	9
KØB	10
DKK	11
123456,78	12
	13
DANKORT	14
PSN: 01	15
XXXX XXXX XXXX XXX6 789	16
TERM: 1F2G3H4I-123456	17
### PBS NR:1234567890	18
	19
	20
ATC:12345	21
AED:000124	22
AID: 0123456789ABCDEF	23
PSAM: 1234567-1234567890	24
ARC:AB	25
STATUS:1234	26
AUT KODE: 1A2B3C	27
REF:123456	28
AUTORISERET	29
	30
	31
	32
	33
	34
	35
	36.1
KORTHOLDERS KOPI	36.2

Figure G.25 – Signature or Combined CVM – Cardholder’s Receipts

### G.5.3 Refund (Signature)

The receipts printed shall be based on the data received/generated during the Business Call:

- Refund

PBS – TESTSHOP	1		
LAUTRUPBJERG 10	2		
2750 BALLERUP	3		
TLF. 44 68 44 68	4		
CVR.NR. 12345678	5		
	6		
2000–06–24	18:15	7	
		8	
RETUR	DKK	123456,78	9
		_____	13
DANKORT	PSN: 01		14
XXXX XXXX XXXX XXX6 789			15
TERM: 1F2G3H4I–123456			16
### PBS NR:1234567890			17
			23
FORRETNINGENS SIGNATUR:			24
			25
			26
			27
.....			28
			29
ATC:12345	AED:000124		30
AID: 0123456789ABCDEF			31
PSAM: 1234567–1234567890			32
ARC:AB	STATUS:1234		33
AUT KODE: 1A2B3C			34
REF:123456	AUTORISERET		35
			36.1
KORTHOLDERS KOPI			36.2

Figure G.26 – Refund (Signature) – Cardholder’s Receipt

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24	7
18:15	8
RETUR DKK 123456,78	9
	13
DANKORT PSN: 01	14
XXXX XXXX XXXX XXX6 789	15
TERM: 1F2G3H4I-123456	16
### PBS NR:1234567890	17
	29
ATC:12345 AED:000124	30
AID: 0123456789ABCDEF	31
PSAM: 1234567-1234567890	32
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF:123456 AUTORISERET	35
	36.1
FORRETNINGENS NOTA	36.2

Figure G.27 – Refund (Signature) – Merchants Receipt

**NOTE:** Merchants receipt may be omitted if the information is stored in the Merchant Application.



## G.5.4 Signature or Combined CVM – Possibility for adding Extra Amount

The receipts printed shall be based on the data received/generated during the Business Call:

- Original Authorization

If the cardholder has increased the amount, and the resulting total amount exceeds the amount covered by the Original Authorization performed, a Supplementary Authorization must be initiated before the transaction process can be completed.

PBS – TESTSHOP	1		
LAUTRUPBJERG 10	2		
2750 BALLERUP	3		
TLF. 44 68 44 68	4		
CVR.NR. 12345678	5		
	6		
2000–06–24	18:15	7	
		8	
KØB	DKK	123456,78	9
EKSTRA	DKK		10
		_____	11
TOTAL	DKK		12
		_____	13
DANKORT	PSN: 01		14
XXXX XXXX XXXX XXX6 789			15
TERM: 1F2G3H4I–123456			16
### PBS NR:1234567890			17
			18
** VED EKSTRA **			19
HUSK NY KVITTERING			20
** WHEN TIPPING **			21
ASK FOR NEW RECEIPT			22
			23
FORRETNINGENS SIGNATUR:			24
			25
			26
			27
.....			28
			29
ATC:12345	AED:000124		30
AID: 0123456789ABCDEF			31
PSAM: 1234567–1234567890			32
ARC:AB	STATUS:1234		33
AUT KODE: 1A2B3C			34
REF:123456	AUTORISERET		35
			36.1
FORRETNINGENS NOTA			36.2

Figure G.28 – Signature or Combined CVM – Possibility for adding Extra Amount – Merchant Receipts



### G.5.5 Signature or Combined CVM – after adding Extra Amount

The receipts printed shall be based on the data received/generated during the Business Call:

- Capture

If no extra amount has been added, the amount printed in line 10 shall be 0,00, and the amount in line 12 shall be equal to the amount in line 9.

PBS – TESTSHOP			1
LAUTRUPBJERG 10			2
2750 BALLERUP			3
TLF. 44 68 44 68			4
CVR.NR. 12345678			5
			6
2000–06–24		18:15	7
			8
KØB	DKK	123456,78	9
EKSTRA	DKK	123,45	10
		_____	11
TOTAL	DKK	123580,23	12
		_____	13
DANKORT		PSN: 01	14
XXXX XXXX XXXX XXX6 789			15
TERM: 1F2G3H4I–123456			16
### PBS NR:1234567890			17
			29
ATC:12345		AED:000124	30
AID: 0123456789ABCDEF			31
PSAM: 1234567–1234567890			32
ARC:AB		STATUS:1234	33
AUT KODE: 1A2B3C			34
REF:123456		AUTORISERET	35
			36.1
		FORRETNINGENS NOTA	36.2

Figure G.30 – Signature or Combined CVM – after adding Extra Amount – Merchant Receipt

**NOTE:** Merchants receipt may be omitted if the information is stored in the Merchant Application, or has already been printed according to step G.5.4 above.



## G.5.6 Original Authorization with PIN or Combined CVM

The receipt printed shall be based on the data received/generated during the Business Call:

- Original Authorization

PBS – TESTSHOP	1		
LAUTRUPBJERG 10	2		
2750 BALLERUP	3		
TLF. 44 68 44 68	4		
CVR.NR. 12345678	5		
	6		
2000–06–24	18:15	7	
		8	
KØB	DKK	123456,78	9
		_____	13
DANKORT	PSN: 01		14
XXXX XXXX XXXX XXX6 789			15
TERM: 1F2G3H4I–123456			16
### PBS NR:1234567890			17
			29
ATC:12345	AED:000124		30
AID: 0123456789ABCDEF			31
PSAM: 1234567–1234567890			32
ARC:AB	STATUS:1234		33
AUT KODE: 1A2B3C			34
REF:123456	AUTORISERET		35
*****			36.1
	KUN AUTORISATION		36.2
*****			36.3
			36.4

Figure G.32 – Original Authorization with PIN or Combined CVM – Cardholder’s Receipt

## G.5.7 Release of Token – Reversal (Authorization)

The receipt printed shall be based on the data received/generated during the Business Call:

- Reversal (Authorization)

If an Original Authorization (and may be one or more Supplementary Authorizations) has been completed, a Token will be available in the terminal equipment.

If the payment process is interrupted, and no concluding Capture will be initiated, the Token shall be released by initiating a Reversal (Authorization).

In this case the cardholder shall be able to receive a receipt showing that the payment process has been interrupted.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6.1
*****	6.2
ANNULLERING (AUT.)	6.3
*****	6.4
	6.5
2000-06-24                    18:15	7
	8
KØB                    DKK  123456,78	9
	13
DANKORT                    PSN: 01	14
XXXX XXXX XXXX XXX6 789	15
TERM:          1F2G3H4I-123456	16
###          PBS NR:1234567890	17
	29
ATC:12345          AED:000124	30
AID:          0123456789ABCDEF	31
PSAM: 1234567-1234567890	32
ARC:AB          STATUS:1234	33
AUT KODE:          1A2B3C	34
REF:123456          AUTORISERET	35
*****	36.1
ANNULLERING (AUT.)	36.2
*****	36.3
	36.4

**NOTE:** The printout of this receipt may await the cardholder's request for the receipt, e.g. in Fuels Dispensers.

### G.5.8 PIN or No CVM – Extra Amount added before Cardholder Acceptance

The receipts printed shall be based on the data received/generated during the Business Call:

- Purchase

If no extra amount has been added, the amount printed in line 10 shall be 0,00, and the amount in line 12 shall be equal to the amount in line 9. Additional line 10 – 12 may be omitted.

PBS – TESTSHOP			1
LAUTRUPBJERG 10			2
2750 BALLERUP			3
TLF. 44 68 44 68			4
CVR.NR. 12345678			5
			6
2000–06–24		18:15	7
			8
KØB	DKK	123456,78	9
EKSTRA	DKK	123,45	10
		_____	11
TOTAL	DKK	123580,23	12
		_____	13
DANKORT		PSN: 01	14
XXXX XXXX XXXX XXX6 789			15
TERM:	1F2G3H4I–123456		16
###	PBS NR:1234567890		17
			29
ATC:12345		AED:000124	30
AID:	0123456789ABCDEF		31
PSAM:	1234567–1234567890		32
ARC:AB		STATUS:1234	33
AUT KODE:		1A2B3C	34
REF:123456		AUTORISERET	35
			36.1
		FORRETNINGENS NOTA	36.2

Figure G.33 – PIN and No CVM – Extra Amount added before Cardholder Acceptance – Cardholder Receipt







## G.6 Receipts – 18 Characters per Line

### G.6.1 General Requirements

This section defines the layout of receipts for printers limited to print a maximum of 18 characters per line.

**NOTE:** An approved waiver for requirement 10.2.11.1 is compulsory.

- G.6.1.1 A If the receipt printer is limited to print a maximum of 18 characters per line, only the following Business Calls shall be supported:
- Purchase (PIN, Signature, No CVM or Combined)
  - Refund
- G.6.1.2 A If the receipt printer is limited to print a maximum of 18 characters per line, the handling of gratuity (or other additional amounts) shall not be supported.
- G.6.1.3 A If the receipt printer is limited to print a maximum of 18 characters per line, a dedicated receipt header (line 1 – 5) shall replace the ‘standard’ header based on 24 characters per line, or the Merchant/Terminal Supplier shall make sure that the ‘standard’ header may be shortened to 18 characters per line.
- G.6.1.4 A The Terminal Supplier shall make sure that the area defined by the lines 25 – 28 is sufficient to enable the cardholder to sign the receipt.

## G.6.2 Standard Layout – 24 Characters per Line

Figure G.36 shows the receipt printed when a standard transaction has been performed successfully and the receipt printer supports 24 characters per line.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000–06–24	7
18:15	8
KØB DKK 123456,78	9
EKSTRA DKK	10
	11
TOTAL DKK	12
	13
DANKORT PSN: 01	14
XXXX XXXX XXXX XXX6 789	15
TERM: 1F2G3H4I–123456	16
I@1 PBS NR:1234567890	17
	18
** VED EKSTRA **	19
HUSK NY KVITTERING	20
** WHEN TIPPING **	21
ASK FOR NEW RECEIPT	22
	23
KORTHOLDERS SIGNATUR:	24
	25
	26
	27
.....	28
	29
ATC:12345 AED:000124	30
AID: 0123456789ABCDEF	31
PSAM: 1234567–1234567890	32
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF:123456 AUTORISERET	35
	36

Figure G.36 – Standard Layout – 24 Characters per Line

### G.6.3 Standard Layout – 18 Characters per Line

- G.6.3.1 A When a standard transaction has been performed successfully and the receipt printer is limited to print a maximum of 18 characters per line, the layout of the receipt shall be as shown in figure G.37.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24 18:15	7
	8
KØB DKK 123456,78	9
	13
DANKORT	14a
PSN: 01.... XXXX	14b
XXXX XXXX XXX6 789	15
TM:1F2G3H4I-123456	16
I@3 PBS:1234567890	17
	23
KORTHOLDERS	24a
SIGNATUR:	24b
	25
	26
	27
.....	28
	29
ATC: 12345	30a
AED: 000124	30b
AID:0123456789ABCD	31a
0123456789ABCDEF01	31b
PSAM:	32a
1234567-1234567890	32b
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF: 123456	35a
AUTORISERET	35b
	36

Figure G.37 – Standard Layout – 18 Characters per Line

- G.6.3.2 A Line 9: For Refund the text ‘KØB DKK’ shall be changed to ‘RETUR DKK’.
- G.6.3.3 A Line 31a/b: If the AID exceeds 14 hexadecimal characters, the AID shall be split in two lines, where the first 14 characters shall be included in line 31a.
- If the AID consists of max 14 hexadecimal characters, line 31b may be omitted.

## G.6.4 Purchase – Based on PIN or No CVM (18 Characters per Line)

- G.6.4.1 A When a Purchase transaction (PIN or No CVM) has been performed successfully and the receipt printer is limited to print a maximum of 18 characters per line, the layout of the receipt shall be as shown in figure G.38.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000–06–24 18:15	7
	8
KØB DKK 123456,78	9
	13
DANKORT	14a
PSN: 01..... XXXX	14b
XXXX XXXX XXX6 789	15
TM:1F2G3H4I–123456	16
IA3 PBS:1234567890	17
	29
ATC: 12345	30a
AED: 000124	30b
AID:0123456789ABCD	31a
0123456789ABCDEF01	31b
PSAM:	32a
1234567–1234567890	32b
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF: 123456	35a
AUTORISERET	35b
	36

Figure G.38 – Purchase – Based on PIN or No CVM  
(18 Characters per Line)

## G.6.5 Purchase – Based on Signature or Combined CVM (18 Characters per Line)

- G.6.5.1 A When a Purchase transaction (Signature or Combined CVM) has been performed successfully and the receipt printer is limited to print a maximum of 18 characters per line, the layout of the receipts shall be as shown in figure G.39.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24 18:15	7
	8
KØB DKK 123456,78	9
_____	13
DANKORT	14a
PSN: 01.... XXXX	14b
XXXX XXXX XXX6 789	15
TM:1F2G3H4I-123456	16
I@3 PBS:1234567890	17
	23
KORTHOLDERS	24a
SIGNATUR:	24b
	25
	26
	27
.....	28
	29
ATC: 12345	30a
AED: 000124	30b
AID:0123456789ABCD	31a
0123456789ABCDEF01	31b
PSAM:	32a
1234567-1234567890	32b
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF: 123456	35a
AUTORISERET	35
	36.1
FORRETNINGENS NOTA	36.2

Figure G.39 – Purchase – Based on Signature or Combined CVM (18 Characters per Line)

The cardholder part of the receipt is shown on the next page.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000–06–24 18:15	7
	8
KØB DKK 123456,78	9
	13
DANKORT	14a
PSN: 01.... XXXX	14b
XXXX XXXX XXX6 789	15
TM:1F2G3H4I–123456	16
I@3 PBS:1234567890	17
	29
ATC: 12345	30a
AED: 000124	30b
AID:0123456789ABCD	31a
0123456789ABCDEF01	31b
PSAM:	32a
1234567–1234567890	32b
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF: 123456	35a
AUTORISERET	35
	36.1
KORTHOLDERS KOPI	36.2

Figure G.39 – Purchase – Based on Signature or Combined CVM (18 Characters per Line) (*concluded*)

## G.6.6 Refund – Based on Signature (18 Characters per Line)

- G.6.6.1 A When a Refund transaction has been performed successfully and the receipt printer is limited to print a maximum of 18 characters per line, the layout of the receipts shall be as shown in figure G.40.

PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000-06-24 18:15	7
	8
RETUR DKK123456,78	9
	13
DANKORT	14a
PSN: 01..... XXXX	14b
XXXX XXXX XXX6 789	15
TM:1F2G3H4I-123456	16
I@5 PBS:1234567890	17
	23
FORRETNINGENS	24a
SIGNATUR:	24b
	25
	26
	27
.....	28
	29
ATC: 12345	30a
AED: 000124	30b
AID:0123456789ABCD	31a
0123456789ABCDEF01	31b
PSAM:	32a
1234567-1234567890	32b
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF: 123456	35a
AUTORISERET	35
	36.1
KORTHOLDERS KOPI	36.2

Figure G.40 – Refund – Based on Signature  
(18 Characters per Line)

The merchant part of the receipt is shown on the next page.



PBS – TESTSHOP	1
LAUTRUPBJERG 10	2
2750 BALLERUP	3
TLF. 44 68 44 68	4
CVR.NR. 12345678	5
	6
2000–06–24 18:15	7
	8
RETUR DKK123456,78	9
	13
DANKORT	14a
PSN: 01.... XXXX	14b
XXXX XXXX XXX6 789	15
TM:1F2G3H4I–123456	16
I@5 PBS:1234567890	17
	29
ATC: 12345	30a
AED: 000124	30b
AID:0123456789ABCD	31a
0123456789ABCDEF01	31b
PSAM:	32a
1234567–1234567890	32b
ARC:AB STATUS:1234	33
AUT KODE: 1A2B3C	34
REF: 123456	35a
AUTORISERET	35
	36.1
FORRETNINGENS NOTA	36.2

Figure G.40 – Refund – Based on Signature  
(18 Characters per Line) (*concluded*)

## G.7 Receipts in English

### G.7.1 General Requirements

In terminals placed where the cardholders mainly are foreigners, the receipts may be translated into English.

- G.7.1.1 A Table G.8 and G.9 defines how Danish text shall be translated into English for printers able to print 24 or 18 characters per line respectively.

Table G.8 – Danish Text Translated into English  
(24 Characters per Line)

24 Characters per Line	
Text	
Danish	English
AFBRUDT – CANCEL	INTERRUPTED – CANCEL
AFBRUDT – FEJL	INTERRUPTED – ERROR
AFVIST	DECLINED
ANNULLERING (AUT)	REVERSAL (AUTH)
AUTORISERET	AUTHORIZED
BEHOLD NOTAEN KOPI TIL KORTHOLDER	RETAIN RECEIPT CARDHOLDER'S COPY
BELØB	AMOUNT
BYTTEPENGE	CASHBACK
EKSTRA	EXTRA
FORRETNINGENS NOTA	MERCHANT'S RECEIPT
GEBYR	FEE
HUSK NY KVITTERING	ASK FOR NEW RECEIPT
KØB	AMOUNT
KOPI	COPY
KORTHOLDERS KOPI	CARDHOLDER'S RECEIPT
KORTHOLDERS SIGNATUR	CARDHOLDER'S SIGNATURE
KUN AUTORISATION	AUTHORIZATION ONLY
KUN TIL INFORMATION:	FOR INFORMATION ONLY:
RETUR	REFUND
SIGNATUR AFVIST	SIGNATURE DECLINED
TOTAL	TOTAL
VED EXTRA	WHEN TIPPING

Table G.9 – Danish Text Translated into English  
(18 Characters per Line)

18 Characters per Line	
Text	
Danish	English
AFBRUDT – CANCEL	INTERRUPTED CANCEL
AFBRUDT – FEJL	INTERRUPTED ERROR
AFVIST	DECLINED
ANNULLERING (AUT)	REVERSAL (AUTH)
AUTORISERET	AUTHORIZED
BEHOLD NOTAEN KOPI TIL KORTHOLDER	RETAIN RECEIPT CARDHOLDER'S COPY
BELØB	AMOUNT
BYTTEPENGE	CASHBACK
EKSTRA	EXTRA
FORRETNINGENS NOTA	MERCHANT'S RECEIPT
GEBYR	FEE
HUSK NY KVITTERING	ASK FOR NEW RECEIPT
KØB	AMOUNT
KOPI	COPY
KORTHOLDERS KOPI	CARDHOLDER'S RECEIPT
KORTHOLDERS SIGNATUR	CARDHOLDER'S SIGNATURE
KUN AUTORISATION	AUTHORIZATION ONLY
KUN TIL INFORMATION:	FOR INFORMATION ONLY:
RETUR	REFUND
SIGNATUR AFVIST	SIGNATURE DECLINED
TOTAL	TOTAL
VED EXTRA	WHEN TIPPING



This page is intentionally left blank

# Attachment H. Privacy Shield on PIN Entry Devices

## H.1 Introduction

The scope of this attachment 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 attachment 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.

### H.1.1 Terminology

<b>Authorized Person,</b>	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.
<b>Card Data,</b>	the complete data contents (track 2) of the magnetic stripe on the Card.
<b>Shoulder Surfing,</b>	the situation when a PIN is compromised as a result of visual pick up while the PIN is entered.
<b>Tapping Device,</b>	a physical device placed in connection with either the PIN Entry Device or the Card Reader for mechanical and/or electronic collection of data.

## H.2 Privacy Shield around the PIN Entry Devices

### H.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.

- H.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 H.1)
- 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.
- H.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 H.2.
- 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 H.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.
- H.2.1.3 A The shielding shall be built in a non-transparent material.
- H.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.

## H.2.2 PIN Entry Device and Numeric Keys

If the terminal includes both a PIN Entry Device and an additional numeric keyboard the layouts shall be strikingly different

to prevent the cardholder from accidentally entering the PIN–code on the numeric keyboard.

- H.2.2.1 B If an additional set of numeric keys (0–9) is included on 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”.

- H.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.

- H.2.2.3 B The additional set of numeric keys shall clearly be marked with the purpose of the use of these keys.

- H.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 “kun PIN–koder” (only PIN–codes).

- H.2.2.5 B A warning saying “Beskyt din PIN–kode” (protect your PIN–code) 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.

- H.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.

## H.3 Shielding – Design Recommendations

### H.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.

- H.3.1.1 C The shielding is only intended to cover the PIN keys – not the command keys, Cancel (Slet Alt), Clear (Slet) and Accept (Godkend).

- H.3.1.2 C The shielding and the cardholder’s body are intended to protect against Shoulder Surfing from all angles.

- H.3.1.3 C The shielding shall allow for use by both right–handed and left–handed cardholders.

- H.3.1.4 C The shielding shall take into account the size of the cardholders hand.

H.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.
H.3.1.6	C	The shielding may not limit the use depending on the light.
H.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.
H.3.1.8	C	The shielding may not limit the operation of the Card Reader, functions key or other operations of the terminal.
H.3.1.9	C	The shielding should be constructed to operate in the environment for which the terminal is intended.
H.3.1.10	C	The shielding should be robust and easy to clean.
H.3.1.11	C	The shielding should be considered as an integrated part of the ‘total design’ of the terminal.
H.3.1.12	C	The design of the shielding should be simple and harmonically.
H.3.1.13	C	The shielding should signal that the use of the terminal is easy and confident.

## H.4 Placement and Installation of the terminal

### H.4.1 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.

### H.4.2 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.

- H.4.2.1 A 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.

- H.4.2.2 C The mounting of the PIN Entry Device should prevent the 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.

## H.5 Placement of the terminal

### H.5.1 Introduction

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.

- H.5.1.1 B 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 H.5)

- H.5.1.2 B 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 H.5)

- H.5.1.3 C It is recommended that the Attended terminal is placed with the PIN Entry Device in a height between 900 and 1000 millimeter.

- H.5.1.4 B 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 H.4).
- H.5.1.5 B When the Unattended terminal is installed as intended the PIN Entry Device shall be in an angle between Horizontal and Vertical (see figure H.4).
- H.5.1.6 C 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

- H.5.1.7 B 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 H.5)

**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.

- H.5.1.8 C 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.

## H.6 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.*

### H.6.1 Access to the inside 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.

- H.6.1.1 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.

- H.6.1.2 B The terminal cabinet shall be locked, even when the terminal is not in use.

- H.6.1.3 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.

- H.6.1.4 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.

- H.6.1.5 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.

- H.6.1.6 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.

- H.6.1.7 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.

- H.6.1.8 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.

## H.6.2 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.

- H.6.2.1 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.

- H.6.2.2 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.

- H.6.2.3 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.

- H.6.2.4 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.

- H.6.2.5 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.

- H.6.2.6 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.

## H.6.3 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.

- H.6.3.1      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.

- H.6.3.2      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 person must not be able to open any switch– or connect–boxes without making damage, if the card data is transmitted through the boxes.

## H.7 Figures

### H.7.1 Privacy Shield around the PIN Entry Device

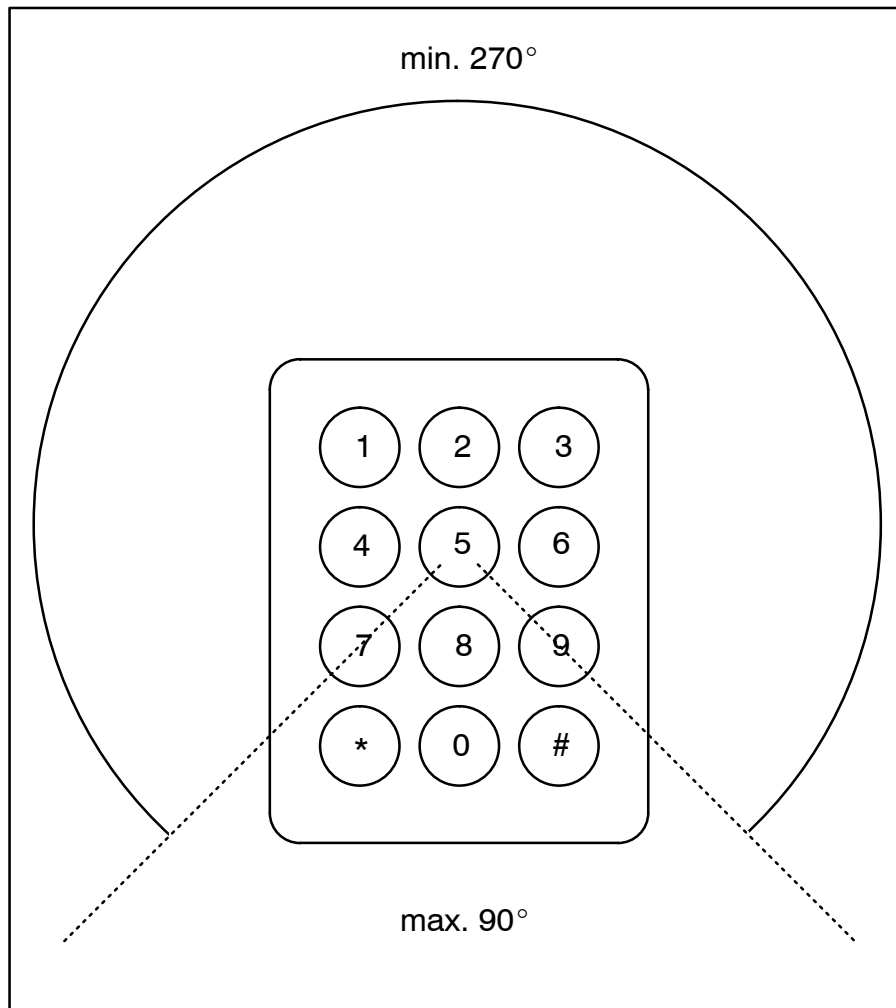


Figure H.1 – Privacy Shield around the PIN Entry Device

## H.7.2 Reference Directions

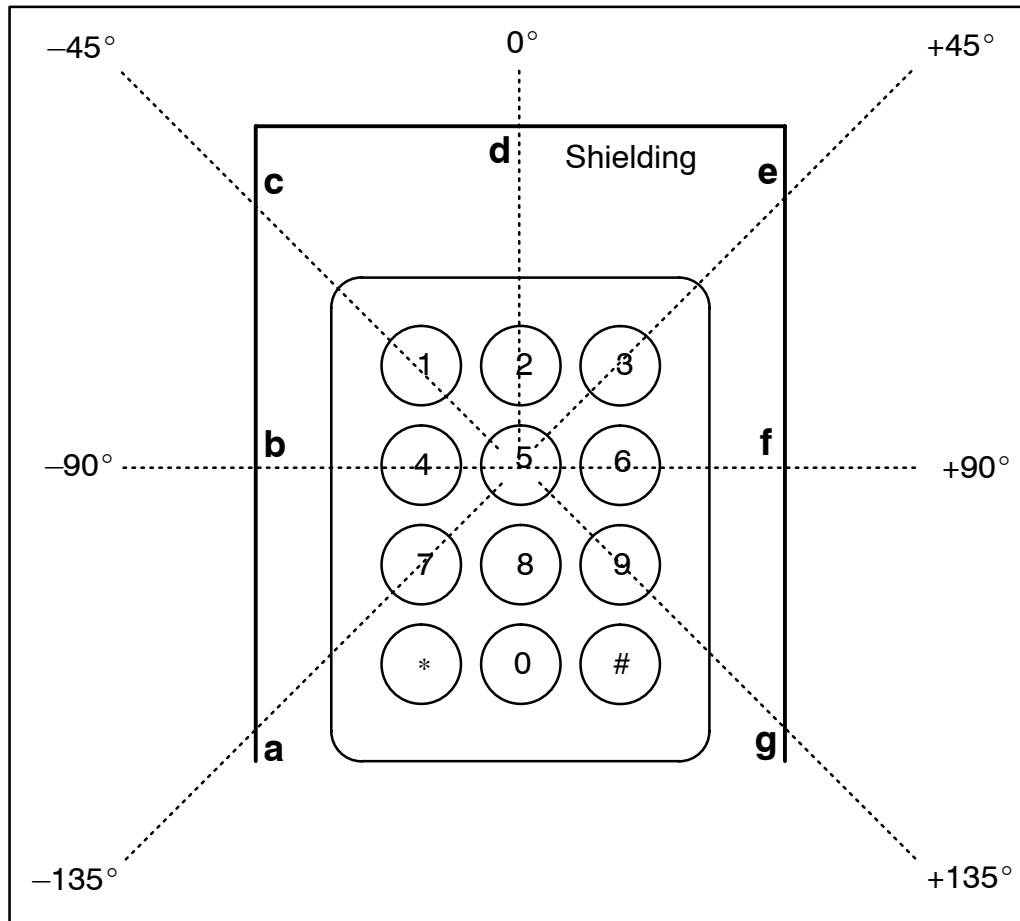


Figure H.2 – Reference Directions – a, b, c, d, e, f and g

### H.7.3 The Height of the Shielding

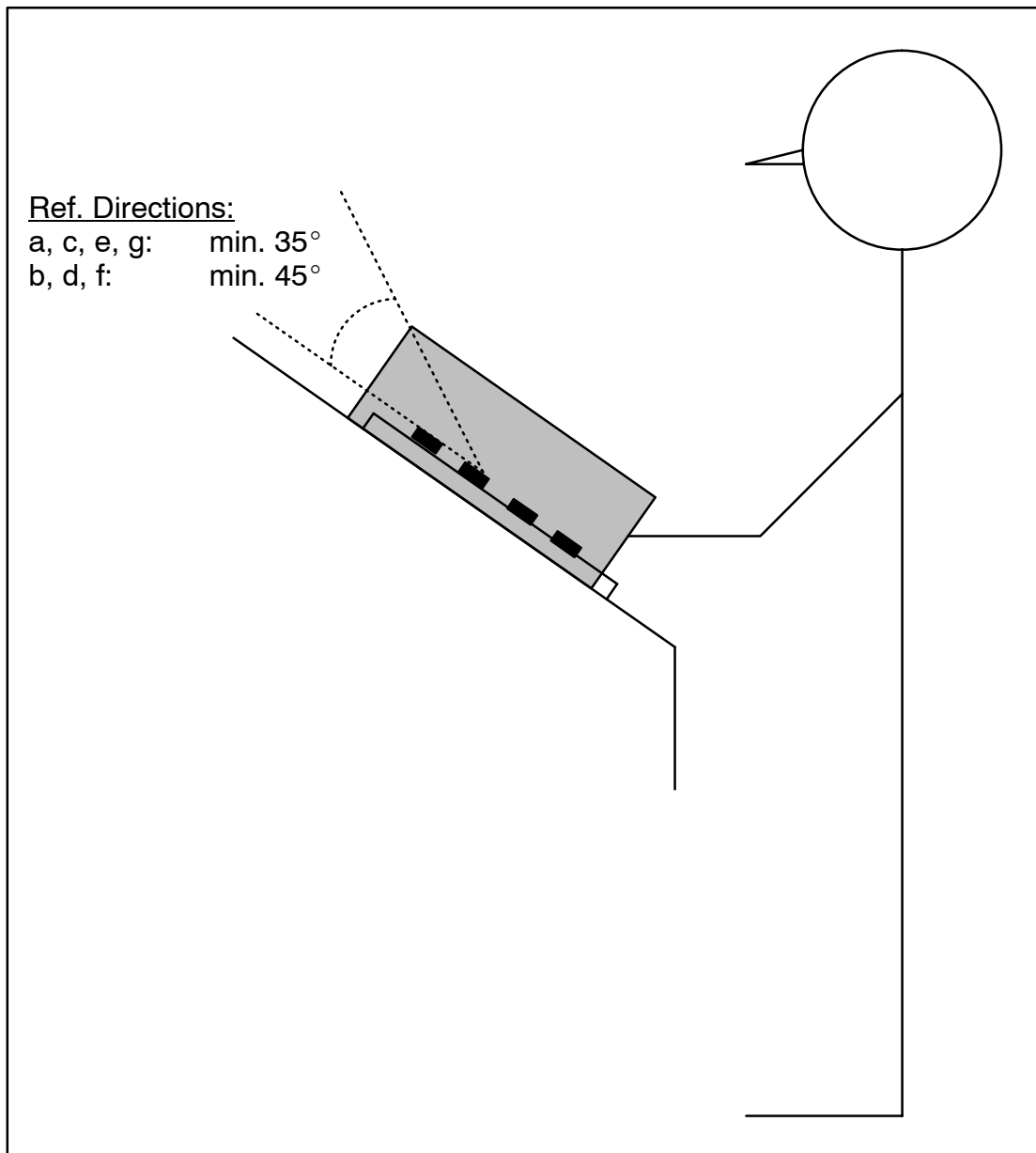


Figure H.3 – The Height of the Shielding



### H.7.4 Mounting of the PIN Entry Device (Angle)

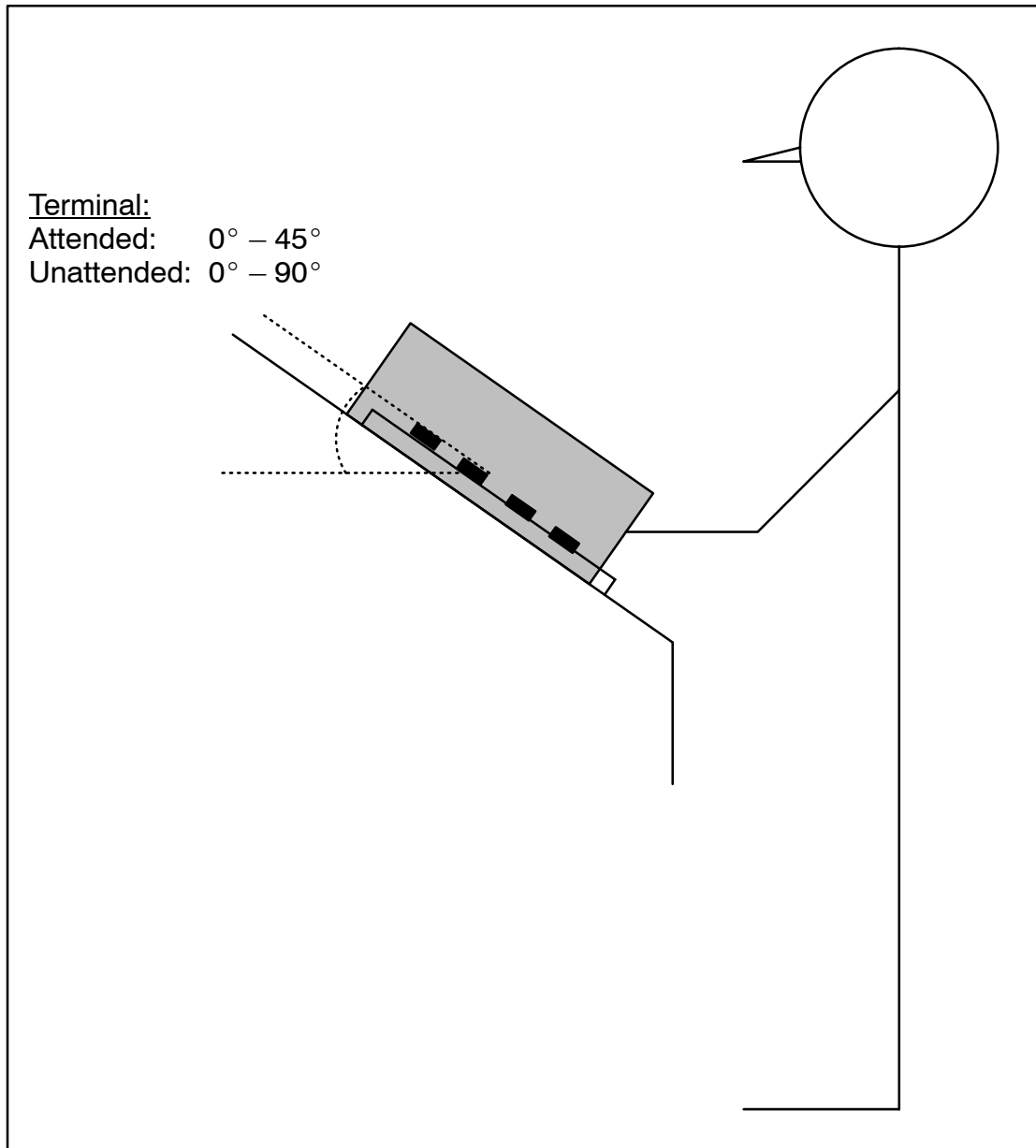


Figure H.4 – Mounting of the PIN Entry Device (Angle)

### H.7.5 Height and position of the PIN Entry Device

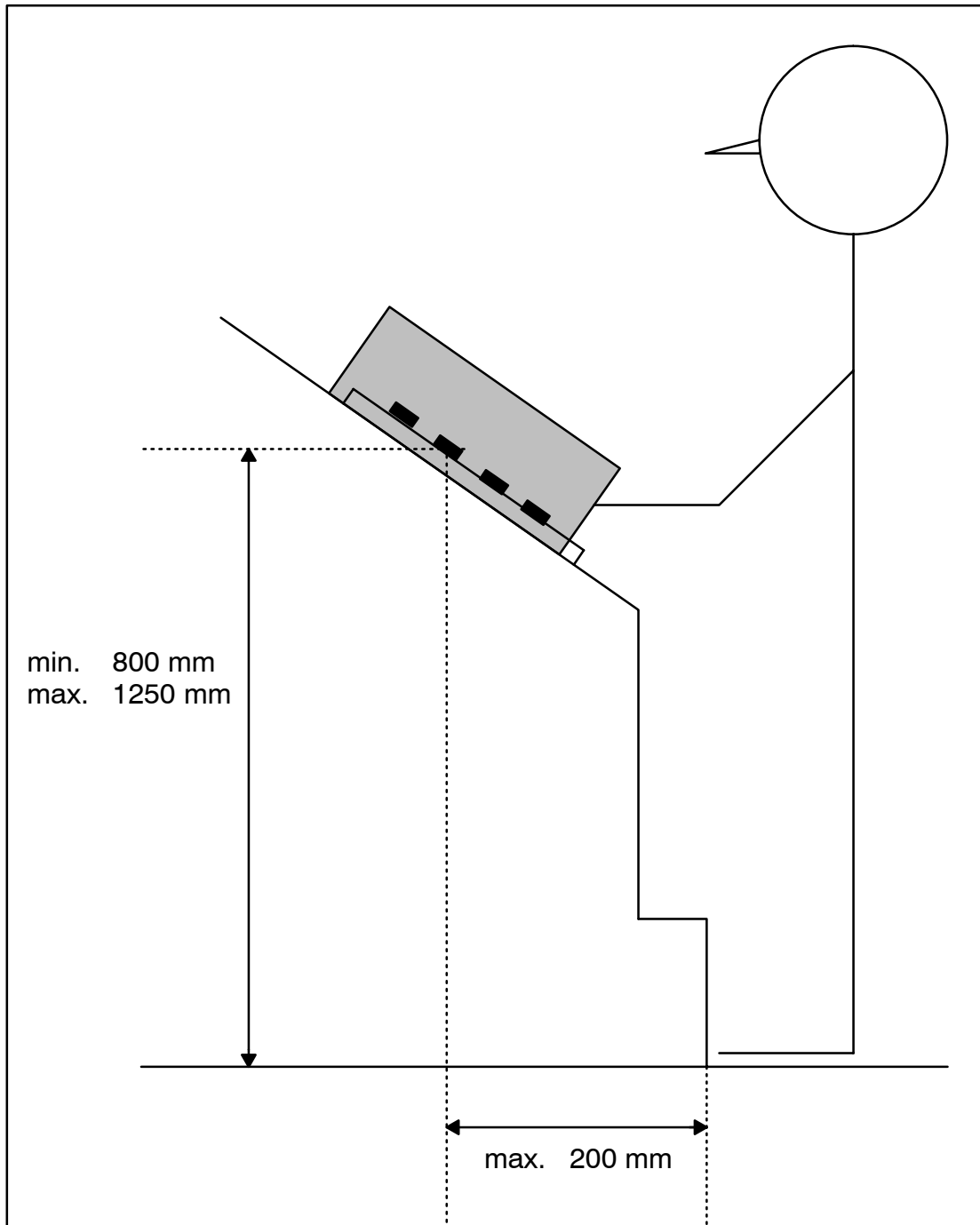


Figure H.5 – Height and Position of the PIN Entry Device

# Attachment I. Gift Voucher / Gavekort

## I.1 Flex Terminals and Gavekort

### I.1.1 Introduction

The scope of this document is to describe

- How to perform Gavekort transactions
- How to get the special Gavekort information

In this document, the name Gavekort is used in connection with using gift vouchers based on magnetic stripe cards in flexterminals.

The details of this document include the information and specifications necessary for implementing functionality for the handling of Gavekort on Flex terminals.

## I.2 Gavekort Transaction Information

The specific Gavekort transaction information is:

- The balance/available funds for the Gavekort
- Expiry Date for the balance/available funds

This information is handled by the terminal in conjunction with the Gavekort application.

## I.3 Accepting Gavekort

The prefix range for Gavekort to be accepted and routed to PBS are sent to the terminal in the response to the *Get MSC Table* command. The command and response for *Get MSC Table* is described in section 8, “Commands and Responses”.

The prefix range to be expected for Gavekort is:  
92086075 – 92086075

Any Gavekort within this range will have 19 digits in the Primary Account Number.

The terminal and cash register needs to have implemented special functionalities for handling Gavekort. The handling of Gavekort takes place exclusively with the merchant, the cardholder hands over the Gavekort card to the merchant.

All parameters concerning Limits, CVM etc. are controlled by the PSAM just as for the usual payment cards.

## I.4 Business Calls for Gavekort Transactions

Table I.1 lists the relations between the business calls initiated on the cash register and the corresponding business calls on the

terminal. Included is an explanation for each business call event as to which actual transactions are initiated.

Table I.1 – Business Calls

Business Call on the Cash Register	Corresponding Business Call on the terminal	Transaction initiated towards PBS
Saldokontrol	Balance Inquiry	An authorization request with an amount of DKK 0,00 Transaction Request = '02' Merchant Initiative = '00' Transaction Type = '00'
Køb	Purchase	A Purchase with a transaction amount equal to the amount to be withdrawn from the Gavekort balance Transaction Request = '00' Merchant Initiative = '00' Transaction Type = '00'
Load	Refund	A Refund with a transaction amount equal to the amount to be loaded onto the Gavekort balance Transaction Request = '01' Merchant Initiative = '00' Transaction Type = '20'
Offline Køb	Offline Purchase	An Offline Purchase with a transaction amount equal to the amount to be withdrawn from the Gavekort balance Transaction Request = '00' Merchant Initiative = '60' Transaction Type = '00'
Offline Load	Refund	An Offline Refund with a transaction amount equal to the amount to be loaded onto the Gavekort balance Transaction Request = '01' Merchant Initiative = '60' Transaction Type = '20'
Køb m. cashback *	Purchase w. cashback	A Purchase with a transaction amount equal to the amount to be withdrawn from the Gavekort balance, 'Amount Other' is used to indicate the cashback amount. Transaction Request = '00' Merchant Initiative = '00' Transaction Type = '09'
<b>Legend:</b> * Køb with cashback is not yet supported.		

## I.5 How to get the Gavekort Transaction Information?

The Terminal need not support any specific service packs in order to handle Gavekort. Accelerated PIN Entry (APE) and Dankort Accelerated PIN Entry (DAPE) may or may not be supported. The transaction amount may or may not be ready at the start of the transaction.

When Gavekort specific information is to be collected by the terminal, the information necessary is to be found in the Issuer Envelope in field 44 tag TY of the response from the Host.

Under tag TY two tags are defined:

- Tag E6 – Balance/Available funds
- Tag M4 – Expiration date for the available funds

Format of the tags are as follows

Table I.2 – 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 (YYMM)

Example: A balance of 1234,56 with an expiration of 2006 January is coded as

54 59 00 10 45 36 00 06 00 00 00 12 34 56 4D 34 00 02 06 01

It is not necessary to send any specific Gavekort information to the Host; the terminal need only follow the transaction flows described in this document.

The necessary Gavekort information is conveyed to the terminal in the Host responses, i.e. the 0116 and 0216 messages. The terminal need to examine the response in order to find the Gavekort specific information.

The general description of the responses can be found in Attachment F, “Host Communication for the Debit/Credit Application – Protocols and Formats”.

If no response from the Host is received on the original request, the terminal shall send a repeat of the request. If no response is received on the repeat request, the transaction is not successful and the PSAM will store a Reversal Advice in the terminal Data Store.

## I.6 Correlation between business and transaction events

The number of flows necessary to perform any business function in connection with Gavekort is determined by regulation and existing procedures in the stores.

It is the cash register attendant who, in the end, must observe that the necessary flows are observed. Neither the cash register nor the terminal need implement functionality for regulating the ‘behaviour’ of the attendant.

As described earlier, the business functions defined for the cash register in connection with Gavekort are:

Saldokontrol, Load, Køb, Offline Køb and Offline Load. Køb with cashback is not yet supported.

- The Saldokontrol is used to perform a balance inquiry for a Gavekort.

- The Load function is used to perform the initial load of funds for a Gavekort, i.e. when ‘selling’ a Gavekort.
- The Køb is used to perform a purchase with the Gavekort.
- The Offline Køb is used to perform a purchase when it is not possible to go online.
- The Offline Load is used to perform the initial load of funds for a Gavekort, i.e. when ‘selling’ a Gavekort, when no on-line transaction is possible.

Two flows are necessary for Gavekort transactions in connection with the common usage of Gavekort in Flex terminals. First a Soldokontrol is performed. If the response indicates that the funds available is sufficient an e.g. purchase can then be initiated.

A Load is performed online such that the cardholder can use the card immediately.

The Saldokontrol is performed using a Balance Inquiry. The Balance Inquiry is actually an authorization request with an ‘Amount’ of DKK 0,00. The Token returned to the terminal shall be discarded by the terminal or the cash register since the Token is not used in the succeeding Køb.

The Køb transaction flow is in two parts. First a Saldokontrol is performed by the merchant. A Køb is then initiated by the merchant if the available funds are sufficient for performing the purchase. The Køb is a standard financial request. The Gavekort account balance and expiration date is returned in the financial request response.

The Offline Køb is performed offline and the financial advice is stored in the terminal data store. The procedure is that the merchant retains the card after an Offline Køb 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 Køb has been performed.

The Offline Load is performed offline which have the consequence that the cardholder cannot use the card immediately. However, as an Advice Transfer is always performed at least at the end of the business day, the advice in the terminal data store is sent to PBS at this time or at an indeterminate time during the same day as part of the usual delivery of advices together with online requests. It is the responsibility of the merchant to inform the cardholder that the card may first be used the following day at the earliest.

It is the responsibility of the merchant to observe the current regulations with regards to any Gavekort balance.

It is always the cash register which determines the Amount and the Track2 Data to be used with any business call initiated from the cash register, i.e. when a Køb is initiated, the cash register must include an Amount and Track2 Data in the call to the terminal.

The following tables describes the transaction flow in connection the defined business functions.

### I.6.1 Balance inquiry

Table I.3 – Balance Inquiry

Event	Terminal – PBS
Merchant swipes or scans the Gavekort Saldokontrol initiated in the cash register	
Terminal initiates a Balance Inquiry	0106 ▶ 1100 0116 ◀ 1110
The balance returned indicates that sufficient funds is available on the Gavekort balance The terminal or the cash register discards the issued Token	

### I.6.2 Loading a Gavekort

Table I.4 – Loading a Gavekort

Event	Terminal – PBS
The merchant initiates and completes a Saldokontrol. If the balance returned indicates that the card account is 'blank', the merchant initiates a Load in the cash register.	
Terminal initiates a Refund with the Amount to be loaded onto the Gavekort	0206 ▶ 1200 0216 ◀ 1210
Load completed OK	

### I.6.3 Buying with a Gavekort

Table I.5 – Buying with a Gavekort

Event	Terminal – PBS
The merchant initiates and completes a Saldokontrol. If the balance returned indicates that sufficient funds is available on the Gavekort balance, a Køb is initiated in the cash register	
Terminal initiates a Purchase with the Amount and Track2 Data received from the cash register.	0206 ▶ 1200 0216 ◀ 1210
Purchase completed OK	

#### I.6.4 Buying with a Gavekort When Online Transactions Cannot Be Performed

Table I.6 – Buying with a Gavekort When Online Transactions Cannot Be Performed

Event	Terminal – PBS
The merchant initiates a Saldokontrol. If no response is received the merchant may then decide to initiate and complete an Offline Køb. The cardholder states an expected balance and the attendant can then choose to trust the cardholder. However, the attendant will usually perform an Offline Køb on the full expected available balance and retain the card after the transaction has taken place.	
Terminal initiates an Offline Purchase with the Amount and Track2 Data received from the cash register.	0226
Purchase completed OK. The financial advice is sent to PBS when possible.	0226 ↗ 1220 0236 ↘ 1230

#### I.6.5 Loading a Gavekort When Online Transactions Cannot Be Performed

Table I.7 – Loading a Gavekort When Online Transactions Cannot Be Performed

Event	Terminal – PBS
The merchant initiates a Saldokontrol. If no response is received the merchant may then decide to initiate and complete an Offline Load. It is the responsibility of the merchant to inform the cardholder that the card may first be used the following day at the earliest.	
Terminal initiates an Offline Refund with the Amount to be loaded onto the Gavekort	0226
Load completed OK The financial advice is sent to PBS when possible.	0226 ↗ 1220 0236 ↘ 1230

### I.7 Dialogue – Merchant and Cardholder

If Gavekort transaction is relevant for the actual transaction, the merchant shall handle the prepaid Gavekort card. This in order to follow existing procedures in the stores. The only action the cardholder is involved in is handing the Gavekort over to the merchant and receiving a receipt after the transaction have taken place.

The merchant either scans the Gavekort, scanning the bar code printed on the card, or swipes the card in a separate card reader. It may be also be swiped on the magnetic stripe card reader on the terminal itself, this however requires a set-up on the counter in which the merchant can easily access the Terminal.



The merchant initiates the relevant business function(s) on the cash register.

The Gavekort specific details, balance and expiration date for the available funds, shall be printed on a receipt. The receipt shall otherwise follow the standard receipt requirements as defined in Attachment G, “Receipts”.

Whenever the merchant performs any transaction using a Gavekort, e.g. a Saldokontrol, a receipt shall be printed.

The following figures describes examples of how the specific Gavekort information shall be added on the otherwise standard receipts.

## 1.8 Error situations

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 file 1.

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 initiate and complete an Advice Transfer.

The terminal shall at least try to deliver any advices stored in files 1 and 2.

The terminal may deliver any advices stored in files 3 and 4.

The automatically initiated Advice Transfer shall take place before any new transaction can be initiated from the cash register.

If the Advice Transfer is not completed successfully, the terminal shall try to perform another Advice Transfer in connection with a new online request.

The Advice Transfer shall be initiated and completed before sending the new online request.

The automatic Advice Transfer shall be performed as described in connection with new online requests until the automatic Advice Transfer has been completed successfully or until a usual Advice Transfer has been initiated and completed successfully.

A PSAM Update Request need not be performed with the automatically initiated Advice Transfer.

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.

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.

In error situations when a receipt is to be printed, the receipts printed shall be without the usual Gavekort specific information.

An example is given in one of the following figures.

## I.9 Receipts

### I.9.1 Receipt for a Køb

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006-05-02		08:42
KØB	DKK	60,00
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I-123456	
DC1	PBS NR:1234567890	
PSAM:	1234567-1234567890	
	STATUS:1234	
AUT KODE:	1A2B3C	
REF:123456	GENNEMFØRT	
SALDO DKK 1234,56		
UDLØBSDATO		2006-12
Specification of service, slogan, clerk etc.		

Figure I.1 – Receipt for a Køb

## I.9.2 Receipt for a Køb with Cashback

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006–05–02		08:42
KØB	DKK	60,00
BYTTEPENGE	DKK	40,00
		<hr/>
TOTAL	DKK	100,00
		<hr/>
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I–123456	
DC1	PBS NR:1234567890	
PSAM:	1234567–1234567890	
	STATUS:1234	
AUT KODE:	1A2B3C	
REF:123456	GENNEMFØRT	
<hr/>		
SALDO	DKK	1234,56
UDLØBSDATO	2006–12	
Specification of service, slogan, clerk etc.		

Figure I.2 – Receipt for a Køb with cashback

**NOTE:** Køb with cashback is not yet supported.

### I.9.3 Receipt for a Saldokontrol

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006-05-02		08:42
BELØB		
		_____
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I-123456	
DC1	PBS NR:1234567890	
PSAM:	1234567-1234567890	
	STATUS:1234	
AUT KODE:	1A2B3C	
REF:123456	AUTORISERET	
*****		
KUN AUTORISATION		
*****		
SALDO	DKK	1234,56
UDLØBSDATO		2006-12
Specification of service, slogan, clerk etc.		

Figure I.3 – Receipt for a Saldokontrol

## I.9.4 Receipt for a Load

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006–05–02		08:42
RETUR	DKK	100,00
		<hr/>
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I–123456	
DC5	PBS NR:1234567890	
PSAM:	1234567–1234567890	
	STATUS:1234	
AUT KODE:	1A2B3C	
REF:123456	GENNEMFØRT	
<hr/>		
SALDO	DKK	100,00
UDLØBSDATO	2006–12	
Specification of service, slogan, clerk etc.		

Figure I.4 – Receipt for a Load

**NOTE:** It is taken for granted that the terminal knows that the receipt is printed for a Gavekort load. Otherwise, two receipts will be printed (as for all other Refund transactions).

## I.9.5 Receipt for an Offline Køb

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006-05-02		08:42
KØB	DKK	60,00
<hr/>		
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I-123456	
DC5	PBS NR:1234567890	
PSAM: 1234567-1234567890		
STATUS:		
REF:123456	AUTORISERET	
<hr/>		
SALDO	DKK	
UDLØBSDATO		
Specification of service, slogan, clerk etc.		

Figure I.5 – Receipt for an Offline Køb

**NOTE:** It is taken for granted that the terminal knows that the receipt is printed for a Gavekort Køb.

## I.9.6 Receipt for an Offline Load

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006–05–02		08:42
RETUR	DKK	100,00
		_____
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I–123456	
DC5	PBS NR:1234567890	
PSAM:	1234567–1234567890	
	STATUS:	
REF:123456	AUTORISERET	
_____		
SALDO	DKK	
UDLØBSDATO		
Specification of service, slogan, clerk etc.		

Figure I.6 – Receipt for an Offline Load

**NOTE:** It is taken for granted that the terminal knows that the receipt is printed for a Gavekort load. Otherwise, two receipts will be printed (as for all other Refund transactions).

### I.9.7 Receipt in case of no Response for a Køb

Specification of service, slogan, clerk etc.		
PBS – TESTSHOP		
LAUTRUPBJERG 10		
2750 BALLERUP		
TLF. 44 68 44 68		
CVR.NR. 12345678		
2006-05-02		08:42
KØB	DKK	60,00
GAVEKORT		
XXXX XXXX XXXX XXX6 789		
TERM:	1F2G3H4I-123456	
DC1	PBS NR:1234567890	
PSAM: 1234567-1234567890		
STATUS:		
*****		
AFBRUDT – FEJL		
*****		
Specification of service, slogan, clerk etc.		

Figure I.7 – Receipt in case of no Response for a Køb

### I.10 Scanning the bar code on the Gavekort vs. using the magnetic stripe

When the magnetic stripe is used, the procedure is as follows.

When the magnetic stripe is swiped in a separate magnetic stripe card reader on the cash register, the cash register must forward the Track2 Data to the terminal. The terminal then processes the transaction as any other transaction with the exception of printing the additional Gavekort information on the receipts.

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 Gavekort information on the receipts.

When the bar code on the Gavekort is scanned, special functionality on the cash register or in the terminal must use the gathered information to construct Track2 Data which can be used to perform the actual transaction.



The general description of a magnetic stripe is found in Attachment A, “Magnetic Stripe Formats”.

Description of the Gavekort Primary Account Number is given in table I.8.

Table I.8 – Primary Account Number

Position	Description	Value
1	National use	9
2 – 4	Country code	208
5	Type – financial application	6
6 – 8	PBS id	075
9 – 11	Customer number	1–999
12 – 18	Serial number	1–9999999
19	Check digit modulus 10, Luhn formula	0–9

Example of a Gavekort Primary Account Number

9 208 6 075 100 0000001 1

Description of data received from the scanned bar code on a Gavekort is given in table I.9.

Table I.9 – 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

Example of data gathered from the scanning of a bar code of a Gavekort

6 075 100 0000001 1 4711

In connection with the construction of Track2 Data of data received from the scanning of a Gavekort, the following applies.

1. The 4 right hand digits of the data obtained from the scanning of the bar code of a Gavekort shall be removed and stored for later use in step 6.
2. The digits 9208 shall be added as the 4 left hand digits.
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 0000702000000 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 in the *Initiate MCS Payment* command.

Example:

1. 6075100000000114711 ▶  
607510000000011
2. 607510000000011 ▶  
9208607510000000011
3. 9208607510000000011
4. 9208607510000000011 ▶  
9208607510000000011D
5. 9208607510000000011D ▶  
9208607510000000011D0000702000000
6. 9208607510000000011D0000702000000 ▶  
9208607510000000011D00007020000004711
7. 9208607510000000011D00007020000004711

As the terminal shall strip the Start Sentinel, LRC and End Sentinel from any magnetic stripe sent to the PSAM in an Initiate MSC Payment, there is no need to include these in the construction of Track2 Data from the data obtained from the scanning of the bar code on the Gavekort.

The coding of Track2 Data is defined in section 9, “Data Elements”.

## I.11 Total Reports

The Gavekort transactions are not settled as transactions performed with traditional payment cards, e.g. Dankort, as Gavekort are prepaid cards with an online balance indicating available funds. There is no settlement between the acquirer and the merchant. In fact there is no acquirer for Gavekort only a processor for the transactions and balancing of the available funds for each Gavekort account.

The merchant however needs to be able to look up the days trade in Gavekort transactions. This total shall appear alongside the usual totals for the payment cards. It is recommended that the Batch Number used for Gavekort transactions is unique and separate from the Batch Numbers used with the conventional payment cards. This in order to easier separate prepaid transactions from normal payment transactions in the Total Report. The Batch Number is indicated, as usual, to the PSAM in the “Payment” command.

It shall be possible for the merchant to differentiate between the number of purchase transactions and refund transactions. It shall also be possible for the merchant to see the number of Load of Gavekort, i.e. the sales of Gavekort.

The merchant may need additional information concerning Gavekort to be available on the Total Report.

# Attachment J. Guidelines for Logging

This Attachment is considered obsolete. Covered by section 5.4.3.

This page is intentionally left blank

# Attachment K. Terms – Business Calls and Administrative Functions

## K.1 Introduction

This attachment provides a translation of the Business Calls and Administrative Functions from English into Danish terms.

## K.2 Business Calls

The following Business Calls are defined in the OTRS specification:

- Purchase
- Refund
- Original Authorization
- Supplementary Authorization
- Reversal (Authorization)
- Capture

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 K.1 defines the names in both English and Danish.

Table K.1 – Business Calls and Service Functions Translated

English	Danish
Purchase	Køb eller Betaling*
Refund	Retur
Original Authorization	Autorisation
Supplementary Authorization	Tillægsautorisation
Reversal (Authorization)	Annuller autorisation
Capture	Efterregistrering
Gratuity or Extra	Ekstra
Cashback	Byttepenge
<b>Legend:</b> * = The most suitable name may be selected.	

## K.3 Administrative Functions

According to the OTRS specifications, the terminal must support a number of Administrative Functions:

- Installation (initiated automatically),
- Advice Transfer,
- Clock Synchronization (may be initiated automatically after other functions),
- PSAM Update Transfer (initiated automatically after other functions),
- PSAM Deactivate.

Based on the names used for similar functions on previous terminal implementations table K.2 defines the names in both English and Danish.

Table K.2 – Administrative Functions Translated

English	Danish
Installation	Installation
Advice Transfer	Afstemning eller Aflevering*
Clock Synchronization	Synkroniser Ur
PSAM Update Transfer	Opdater PSAM
PSAM Deactivate	Afmeld PSAM
<b>Legend:</b> * = The most suitable name may be selected.	

# Attachment L. Defective Advices in Data Store

## L.1 Introduction

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 records stored in the Data Store shall be transferred to the host systems, one-by-one, initiated by the function called Advice Transfer or other similar functions.

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 (e.g. the host rejects the record or the check value received does not match), the terminal application shall not delete the corresponding record from Data Store.

Records which can not be deleted automatically will remain in the Data Store ‘forever’.

This attachment defines additional guidelines concerning manual erasure of such ‘defective records’.

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 6.1.3) can be helpful if problems is detected in the Data Store.

## L.2 Requirements and Principles for the Solution

### L.2.1 General

If the conditions for deleting records from the Data Store are not fulfilled, such ‘defective records’ will remain in the Data Store.

This specification defines by the following requirements the handling of this situation:

Requirement 6.18.7.2: If an Advice is not accepted by the host, the terminal shall try to re–send the Advice twice, before handling the next Advice in the files.

Requirement 6.18.7.3: If the Data Store contains not accepted Advices after the Advice Transfer, a technician shall be alerted. The terminal shall not initiate further Debit/Credit transactions.

Similar situations may occur if the Check Value received, as part of the response from the host, does not match the corresponding value saved 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.

### L.2.2 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.

File-5 file shall be created by the terminal application. The PSAM only requests the creation of File-1 to File-4.

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).

### L.2.3 Adding records to File-5

If a record from File-1 to File-4 has been re-sent the number of times defined, but the host response did not allow the terminal application to delete the record, the record may be moved to File-5 (and deleted from the original file).

The terminal application must assure that communication problems are not the reason why the terminal application has not been allowed to delete the original record from the Data Store.

Since the host systems may omit responding to a ‘defective record’ (due to e.g. security aspects), the terminal application shall initiate at least 3 calls for Advice Transfer (without detecting any communication problems other than ‘no response’ to the concerned record) before moving the record to File-5.

When a record is moved to File-5, additional information shall be saved together with the original record data.

The additional information saved shall as a minimum cover:

- information indicating the original file (File-1 to File-4)
- date and time for adding record to File-5.
- why has the record been added to File-5 (e.g. no host response, wrong check value, Action Code).

When a ‘defective record’ has been moved to File-5, the Advice Transfer may be completed and the remaining records from File-1 to File-4 may be transferred to the host systems and subsequently deleted from these files.

### L.2.4 Transfer of records from File-5

If File-5 contains any records, the terminal application shall be able to empty this file similarly to the flow when File-1 to File-4 are cleared.



If File–5 contains any records, the terminal shall not initiate further Debit/Credit transactions. Advice Transfer (or other administrative functions) may be initiated in this state.

The terminal must indicate that technical support shall be requested.

The technical support shall be carried out by the Terminal Supplier.

## **L.2.5 Deleting records from File–5**

Only the Terminal Supplier shall be able to control the erasure of records from File–5, and it shall only be possible to delete records from File–5.

The Terminal Supplier may use a key–entered ‘dynamic password’ as the key to control the erasure of records. Alternatively, a communication link between the Terminal Supplier’s support system and the terminal may be established to control the erasure.

An Advice Transfer to the host systems covering all records stored in File–5 shall be attempted before the Terminal Supplier may erase any records.

All records stored in File–5 shall be re–send the specified number of times (a total of 3 times), to eliminate the possibility that any of the records could be accepted anyway.

The information stored in a record in File–5 shall be logged before the concerned record may be deleted.

The requirements for the information logged and for the log techniques accepted, are stated below.

## **L.2.6 Log–information, when a record is deleted from File–5**

Before a record may be deleted from File–5, information about the concerned record shall be logged.

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).

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.

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.

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 shall make 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.

The log-information covering records deleted from File-5 shall be transferred to the Terminal Supplier for further investigation and registration.

The general terminal-log (or journal) covering all transactions in the relevant settlement period shall 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.

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.

If a corrected record is re-send from the Terminal Supplier's support system, the function shall be defined as part of the procedures for message and information exchange.

### **L.3 Temporary use while records in File-5**

As stated above, the terminal shall not be able to initiate any further transactions, as long as the terminal contains defective advices (i.e. as long as any records are stored in File-5).

In this situation the terminal will not be able to service new customers, which may be rather inconvenient for both the merchant and the cardholder.

To overcome this problem, the technician or the merchant may be able to resume the service of new customers temporarily, even if records are stored in File-5. A number of conditions must be fulfilled if a terminal shall be re-opened in this situation:

- Re-opening of the terminal (after technical support has been requested due to defective advices) shall only be possible after entry of the merchant password or similar (or higher) security barriers.

- After re-opening of the terminal, the merchant display shall show a message indicating that technical support is required. The message shall at least be displayed when the terminal is in idle state, waiting for the next customer.
- After re-opening of the terminal, the normal/usual transfer of new advices shall not be limited due to the ‘defective but accepted’ advices already stored in File-5.
- If a new defective advice is discovered, after re-opening of the terminal, no further transactions shall be initiated and technical support shall be requested again. After the detection of each new defective advice, a technician (or the merchant) shall be requested and the procedures for re-opening shall be carried out before new transactions shall be initiated.
- Each time a new Advice Transfer is initiated, the transfer shall cover all advices store in the terminal, including all defective advices (stored in File-5).

The above mentioned principles for temporary use of the terminal, even if the terminal contains defective advices, apply to attended terminals.

Similar principles may be used for unattended terminals, but no merchant/sales-assistant will be present, and therefore no person will continuously be advised about the current problem.

The implementation for unattended terminals may depend on the actual type of business and the actual environment.

The implementation may e.g. include an automatic call to a helpdesk (e.g. the terminal suppliers helpdesk) each time a new defective advice is discovered. This call may alert a technician, who shall be able to determine whether further transactions shall be allowed (i.e. terminal shall be re-opened) or the terminal shall be closed due to ‘out of order’.

A pre-approval of the chosen principles for unattended terminal shall be obtained from PBS.

This page is intentionally left blank

# Attachment M. Guidelines for Usage of the User Interface Display

## M.1 Introduction

During the development of terminal implementations, some guidelines or examples concerning how to design the message flow on the User Interface Display may be helpful.

This attachment shows in a number of examples how the message flow on the User Interface Display may be implemented.

This attachment also shows examples for the texts to be displayed, if the terminal is able to display only 16 characters per line.

All the texts stated and all the display flows shown in this attachment shall only be interpreted as examples and guidelines.

If any disagreements are found between the requirements defined elsewhere in the specifications and the examples shown in the present attachment, the requirements defined elsewhere in the specifications shall be considered as the requirements in force.

## M.2 Messages for Display based on 16 Characters per Line

In this section, Messages for Display and Printing is shown.

The texts stated in table M.1 are designed for a display able to show at least 20 characters per line and 16 characters per line respectively.

Table M.1 – Messages for Display and Printing

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 magnet-kortlæser	Use MAG Stripe	Brug magnetkort
'13'	Try Again	Prøv igen	Try Again	Prøv igen
<b>'14' – '3F'</b>	<b>RFU for assignment by EMV</b>			
'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	Annulér	Cancel	Annulér
'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

Table M.1 – Messages for Display and Printing (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'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
'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

Table M.1 – Messages for Display and Printing (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'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 Nr	Auth. X.25 Nr	Auth X25 Nr	Auth. X.25 Nr
'7D'	Upload X25 Nr	Afsendelses X.25 Nr	Upload X25 Nr	Afsend. X.25 Nr
'7E'	Nr Trials:	Nr forsøg	Nr 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	Annulering	Cancellation	Annulering
'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 i base
'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	Ingen kortnummer	No card number	Ingen kortnummer
'98'	Excessive Amount	For højt beløb	Excessive Amount	For højt beløb
'99'	Counterfeit Card	Falsk kort	Counterfeit Card	Falsk kort



Table M.1 – Messages for Display and Printing (*continued*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'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
<b>'B0' – 'DF'</b>	<b>RFU for assignment by TAPA</b>			
'E0'	Terminal ready	Terminalen er klar	Terminal ready	Terminal er klar
'E1' <sup>1)</sup>	No receipt	Ingen kvittering	No receipt	Ingen kvittering
'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:

Table M.1 – Messages for Display and Printing (*concluded*)

Message Code	20 Characters Display		16 Characters Display	
	English	Danish	English	Danish
'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 er 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	Kort/beløb 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:** <sup>1)</sup> The message may flash on the display to attract the cardholder's attention.  
<sup>2)</sup> 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

### M.3 Display flow for Transactions

This section shows how the guiding text messages may be setup 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 20 characters.

It is suggested that the following two unassigned Message Codes, 'EC' and 'F1', are used as follows:

'EC' = “Tast PIN og Godkend” (“Enter PIN and Accept”)

and

'F1' = “Tast Godkend” (“Accept?”).

Message Code '09' may be displayed as either “Indtast PIN” or “Tast PIN”.

Requirement 6.7.1.11 is presumed not be fulfilled!

### M.3.1 Example 1: Display flow for PIN Transaction – 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:	Tast PIN	MC = ‘09’

Figure M.1 – PIN entry enabled but Amount not available yet

#### Step 2 – PIN Entry enabled and Amount available

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = ‘F0’ + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = ‘EF’ + an “*” for each digit entered
Line 3:		
Line 4:	Tast PIN og Godkend	MC = ‘EC’

Figure M.2 – PIN entry enabled and amount available

#### Step 3 – PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = ‘F0’ + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = ‘EF’ + an “*” for each digit entered
Line 3:		
Line 4:	Vent	MC = ‘0E’

Figure M.3 – PIN entry completed and Amount accepted, waiting for Validation

#### Step 4 – Validation completed, Transaction approved

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = ‘F0’ + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = ‘EF’ + an “*” for each digit entered
Line 3:	Godkendt	MC = ‘03’
Line 4:		

Figure M.4 – Validation completed, Transaction approved

### M.3.2 Example 2: Display flow for PIN Transaction – 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:	Tast PIN	MC = '09'

Figure M.5 – PIN entry enabled but Amount not available yet

#### Step 2 – PIN Entry enabled and Amount available

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Tast PIN og Godkend	MC = 'EC'

Figure M.6 – PIN Entry enabled and Amount available

#### Step 3 – PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Vent	MC = '0E'

Figure M.7 – PIN Entry completed and Amount accepted, waiting for Validation

#### Step 4 – Validation completed, Transaction rejected – PIN Error

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:	Afvist	MC = '07'
Line 4:	Forkert PIN	MC = '0A'

Figure M.8 – Validation completed, Transaction rejected – PIN Error

### M.3.3 Example 3: Display flow for PIN Transaction – PIN Error with 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:	Tast PIN	MC = ‘09’

Figure M.9 – PIN entry enabled but Amount not available yet

#### Step 2 – PIN Entry Enabled and Amount available

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = ‘F0’ + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = ‘EF’ + an “*” for each digit entered
Line 3:		
Line 4:	Tast PIN og Godkend	MC = ‘EC’

Figure M.10 – PIN entry enabled and Amount available

#### Step 3 – PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = ‘F0’ + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = ‘EF’ + an “*” for each digit entered
Line 3:		
Line 4:	Vent	MC = ‘0E’

Figure M.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:	KØB: 123456,78 DKK	MC = ‘F0’ + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = ‘EF’ + an “*” for each digit entered
Line 3:	Afvist	MC = ‘07’
Line 4:	Forkert PIN	MC = ‘0A’

Figure M.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:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN:	MC = 'EF' + an "*" for each digit entered
Line 3:	(X) PIN forsøg igen	MC = 'F8', (X) indicates the number of PIN tries left
Line 4a:	Forkert PIN	MC = '0A', alternating between line 4a and 4b
Line 4b:	Tast PIN og Godkend	MC = 'EC', alternating between line 4a and 4b

Figure M.13 – Validation completed, Transaction rejected – PIN Error – (Remaining PIN attempts available – PIN Retry)

### Step 6 – When Cardholder enters the first Digit

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *	MC = 'EF' + an "*" for each digit entered
Line 3:	(X) PIN forsøg igen	MC = 'F8', (X) indicates the number of PIN tries left
Line 4:	Tast PIN og Godkend	MC = 'EC'

Figure M.14 – When the cardholder enters the first PIN Digit

### Step 7 – PIN Entry completed and Amount accepted, waiting for Validation

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	PIN: *****	MC = 'EF' + an "*" for each digit entered
Line 3:		
Line 4:	Vent	MC = '0E'

Figure M.15 – PIN Entry Completed and Amount accepted, waiting for Validation  
and so on.....

### M.3.4 Example 4: Display flow for Signature Transaction – Approved

This example is based on ‘No Amount Acceptance’.

#### Step 1 – Amount available, waiting for Validation

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:		
Line 4:	Vent	MC = '0E'

Figure M.16 – Amount available, waiting for Validation

#### Step 2 – Validation completed, Transaction approved

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:	Godkendt	MC = '03'
Line 4:		

Figure M.17 – Validation completed, Transaction approved

### M.3.5 Example 5: Display flow for signature Transaction – Approved

This example is based on ‘Amount Acceptance’.

#### Step 1 – Amount available, waiting for Cardholder Acceptance

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:		
Line 4:	Tast Godkend	MC = 'F1'

Figure M.18 – Amount available, waiting for cardholder Acceptance

#### Step 2 – Waiting for Validation

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:		
Line 4:	Vent	MC = '0E'

Figure M.19 – Waiting for Validation

#### Step 3 – Validation completed, Transaction approved

	12345678901234567890	
Line 1:	KØB: 123456,78 DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:		
Line 3:	Godkendt	MC = '03'
Line 4:		

Figure M.20 – Validation completed, Transaction approved



## M.4 Display flow for Transactions – max. 16 Characters per Line

This section shows how the guiding text messages may be setup 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.

It is suggested that the following two unassigned Message Codes, 'EC' and 'F1', are used as follows:

'EC' = "Tast PIN og Godkend" ("Enter PIN and Accept")

and

'F1' = "Tast Godkend" ("Accept?").

Message Code 'EC' in 16 character version:

'EC' = "Tast PIN/Godkend" ("Enter PIN/Accept").

Message Code '09' may be displayed as either "Indtast PIN" or "Tast PIN".

Requirements 5.6.4.19 and 5.6.4.24 are presumed not be fulfilled!

### M.4.1 Example 1: Display flow for PIN Transaction – 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:	Tast PIN	MC = '09'

Figure M.21 – PIN entry enabled but Amount not available yet

#### Step 2 – PIN Entry Enabled and Amount available

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Tast PIN/Godkend	MC = 'EC'

Figure M.22 – PIN entry enabled and amount available

#### Step 3 – PIN Entry completed and Amount accepted, waiting for Validation

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	
Line 4:	Vent	MC = '0E'

Figure M.23 – PIN entry completed and Amount accepted, waiting for Validation

#### Step 4 – Validation completed, Transaction approved

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Godkendt	MC = '03'

Figure M.24 – Validation completed, Transaction approved

## M.4.2 Example 2: Display flow for PIN Transaction – 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:	Tast PIN	MC = '09'

Figure M.25 – PIN entry enabled but Amount not available yet

### Step 2 – PIN Entry Enabled and Amount available

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Tast PIN/Godkend	MC = 'EC'

Figure M.26 – PIN entry enabled and amount available

### Step 3 – PIN Entry Completed and Amount Accepted, Waiting for Validation

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Vent	MC = '0E'

Figure M.27 – PIN entry completed and Amount accepted, waiting for Validation

### Step 4 – Validation completed, Transaction rejected – PIN Error

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	Afvist	MC = '07'
Line 4:	Forkert PIN	MC = '0A'

Figure M.28 – Validation completed, Transaction rejected – PIN Error

### M.4.3 Example 3: Display flow for PIN Transaction – PIN Error with 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:	Tast PIN	MC = ‘09’

Figure M.29 – PIN entry enabled but Amount not available yet

#### Step 2 – PIN Entry Enabled and Amount available

	1234567890123456	
Line 1:	KØB: DKK	MC = ‘F0’ + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = ‘EF’ + an “*” for each digit entered
Line 4:	Tast PIN/Godkend	MC = ‘EC’

Figure M.30 – PIN entry enabled and Amount available

#### Step 3 – PIN Entry completed and Amount accepted, waiting for Validation

	1234567890123456	
Line 1:	KØB: DKK	MC = ‘F0’ + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = ‘EF’ + an “*” for each digit entered
Line 4:	Vent	MC = ‘0E’

Figure M.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:	KØB: DKK	MC = ‘F0’ +Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	Afvist	MC = ‘07’
Line 4:	Forkert PIN	MC = ‘0A’

Figure M.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:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	X PINforsøg igen	MC = 'F8', (X) indicates the number of PIN tries left
Line 4a:	Forkert PIN	MC = '0A', alternating between line 4a and 4b
Line 4b:	Tast PIN/Godkend	MC = 'EC', alternating between line 4a and 4b

Figure M.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:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *	MC = 'EF' + an "*" for each digit entered
Line 4:	Tast PIN/Godkend	MC = 'EC'

Figure M.34 – When the cardholder enters the first PIN Digit

### Step 7 – PIN Entry completed and Amount accepted, waiting for Validation

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:	PIN *****	MC = 'EF' + an "*" for each digit entered
Line 4:	Vent	MC = '0E'

Figure M.35 – PIN Entry completed and Amount accepted, waiting for Validation  
and so on.....

#### M.4.4 Example 4: Display flow for Signature – Approved

This example is based on ‘No Amount Acceptance’.

##### Step 1 – Amount available, waiting for Validation

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Vent	MC = '0E'

Figure M.36 – Amount available, waiting for Validation

##### Step 2 – Validation completed, Transaction approved

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Godkendt	MC = '03'

Figure M.37 – Validation completed, Transaction approved

### M.4.5 Example 5: Display flow for Signatue Transaction – Approved

This example is based on ‘Amount Acceptance’.

#### Step 1 – Amount available, waiting for Cardholder acceptance

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Tast Godkend	MC = 'F1'

Figure M.38 – Amount available, waiting for cardholder acceptance

#### Step 2 – Waiting for Validation

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Vent	MC = '0E'

Figure M.39 – Waiting for Validation

#### Step 3 – Validation completed, Transaction approved

	1234567890123456	
Line 1:	KØB: DKK	MC = 'F0' + the Amount + Currency Code (in alpha)
Line 2:	123456,78	The Amount
Line 3:		
Line 4:	Godkendt	MC = '03'

Figure M.40 – Validation completed, Transaction approved

This page is intentionally left blank



# Attachment N. Guidelines for Constructing Total Reports

## N.1 Introduction

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

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

All the information stated in this attachment shall only be interpreted as examples and guidelines.

If any disagreements are found between the requirements defined elsewhere in the specifications and the information stated in the present attachment, the requirements defined elsewhere in the specifications shall be considered as the requirements in force.

## N.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 of constructing a total report. How and when individual transactions and/or a batch of transactions are settled is dependant upon the contracts agreed between the acquirers and the merchant.

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.

## N.3 Data Elements

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

Table N.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 makes out and sends 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 the 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.

## **N.4 Example**

Below is given an example of how some of the (relevant) data elements could be used to make out 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’ printout the acquirers makes out:

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

It is also assumed that the merchant accepts:

- Dankort,
- MasterCard and,
- Diners.

Table N.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
	C05 (DINERS)	020122	001
			002
2	C03 (MASTERCARD)	020121	001
			002
			003
			004
	C05 (DINERS)	020122	001
			002

The transactions are bunched together in batches by the terminal equipment.

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 out *after* all advices have been transferred (i.e. an Advice Transfer has taken place).

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 balancing 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.

## **N.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 Flex 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 N.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

### N.5.1 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 proposal 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 N.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			
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.

## N.5.2 Initialization

Each time a new transaction with financial impact (Purchase, Refund and 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 Report may be ‘released’ again.

### N.5.3 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, then no data elements can be extracted and filled into the Transaction Record.

#### **N.5.4 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 section N.5.1, 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.

#### **N.5.5 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.

The transfer of advices may either be performed during online requests or during a ‘batch transfer’.

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, then no data shall be extracted from the response.

### N.5.6 Result – ‘OK’ or ‘Not OK’

When the transaction sequence, including transfer of belonging advices, 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 have 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 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 trans-

ferred successfully, the corresponding fields defining the reconciliation information must remain ‘empty’.

### **N.5.7 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.

This page is intentionally left blank

# Attachment O. Merchant Initiative Bypass

## O.1 Introduction

Merchant Initiative Bypass is a functionality supported by the OTRS, which makes it possible for the merchant to “force” a certain CVM (PIN, signature or No CVM) or alternatively on-line/offline when a transaction is already 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.

Implementing Merchant Initiative Bypass functionality has only impact on the terminal.

Figure O.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.

## O.2 General

### O.2.1 General Requirements

If the Merchant Initiative Bypass functionality is going to be implemented, the implementation must comply to the following requirements:

- |         |   |   |
|---------|---|---|
| O.2.1.1 | C | When Merchant Initiative Bypass is initiated, the current transaction in progress shall be interrupted as if the merchant activated the Cancel Key.   |
| O.2.1.2 | C | Merchant Initiative Bypass shall only be possible while the <i>Initiate Payment</i> command is in progress.   |
| O.2.1.3 | C | When Merchant Initiative Bypass is initiated, the cardholder shall be informed (via the cardholder display) that the transaction is not rejected, but continues.  |
| O.2.1.4 | C | Taken requirement O.2.1.3 into account, the Message Code ‘87’ (“Cancellation”) shall be substituted by the Message Code ‘64’ (“Retrying”).  |
| O.2.1.5 | 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.  |
| O.2.1.6 | 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 O.1, application selection can be “skipped” in the following way: <ul style="list-style-type: none"><li>• Creation of the Candidate List can be skipped (the existing Candidate List is still valid)</li><li>• The terminal can directly select the application previously selected.</li></ul> |

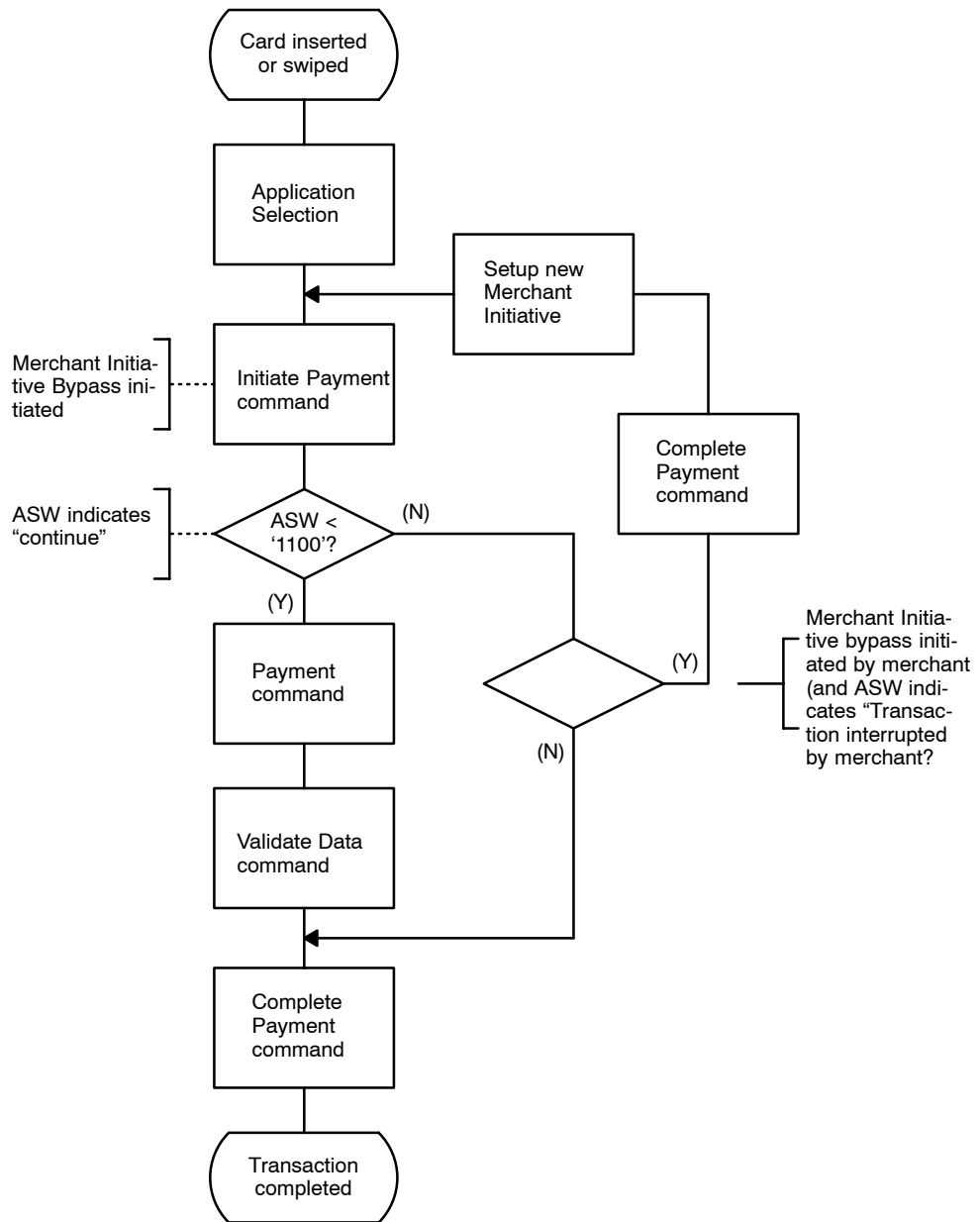


Figure O.1 – Merchant Initiative Bypass

This page is intentionally left blank



# Attachment P. Local PIN

## P.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.

## P.2 Business Requirements

Local PIN described in this attachment 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 PBS.
- The Local PIN functionality shall be independent of card technology.

## P.3 Description

The Local PIN Validation function shall be called from a separate application within the terminal, i.e. an application separate from the ‘PBS debit/credit application’.

As Local PIN is handled by the PSAM for the PBS debit/credit application, the ID<sub>PSAMAPP</sub> has to be ‘8111’ when addressing the PBS PSAM.

The application using the Local PIN functionality shall make this conversion of ID<sub>PSAMAPP</sub> when addressing the PBS PSAM. See example given in figure P.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.

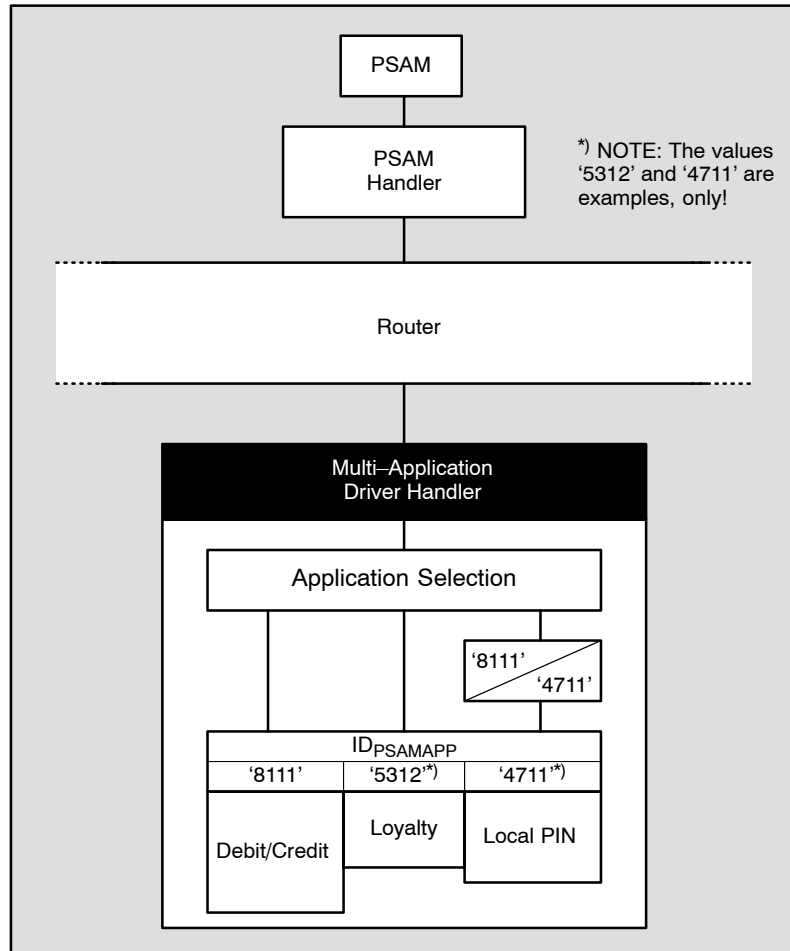
The messages displayed to the cardholder will be the same as used for PIN entry sequences for debit/credit transactions.

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 P.1 – TAPA Architecture



## P.4 Local PIN Validation Message Flow

### P.4.1 Local PIN Validation

#### Validation Flow

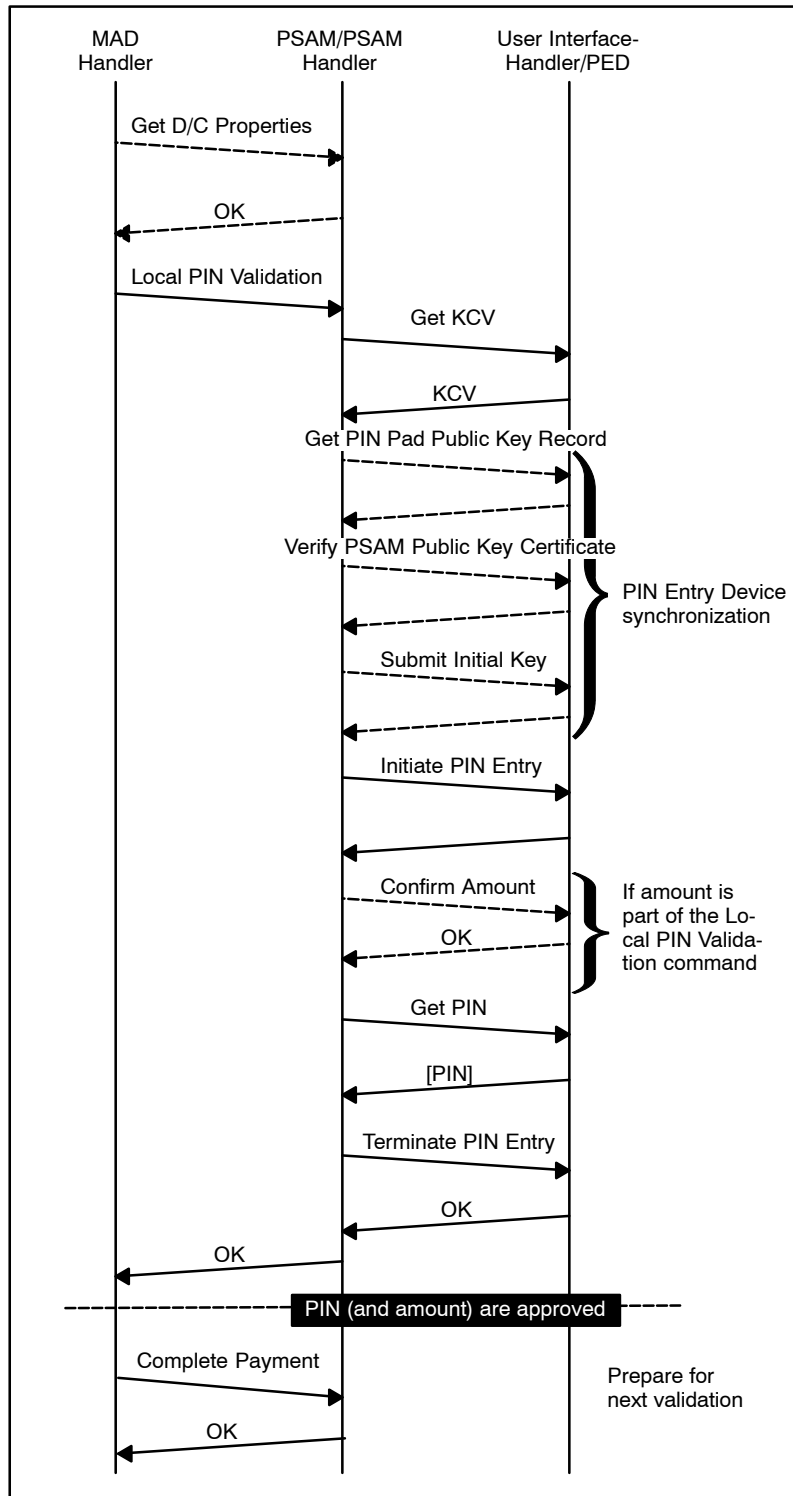
Figure P.2 shows the validation flow for a successful Local PIN Validation. If the *Get KCV* command indicates that a synchronization of the PSAM/PIN Entry Device is required, the synchronization process known from the Debit/Credit application will be applied by the PSAM.

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 P.2 – Local PIN Validation Message Flow



**NOTE:** See also section P.10 for an example of message flow.

## P.5 Plaintext PIN Data

### P.5.1 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.

- P.5.1.1 A The *Local PIN Validation* command sent to the PSAM shall have the format shown in table 8.100.

The response to *Local PIN Validation* command will have the format shown in table 8.101.

- P.5.1.2 A The plaintext PIN block shall be formatted as described in figure P.3.

Figure P.3 – Plaintext PIN Block

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'

This PIN Block format is identical to the PIN block format defined in ref. 36: "EMV, version 4.1" for 'plaintext offline PIN block' in the *Verify* command.

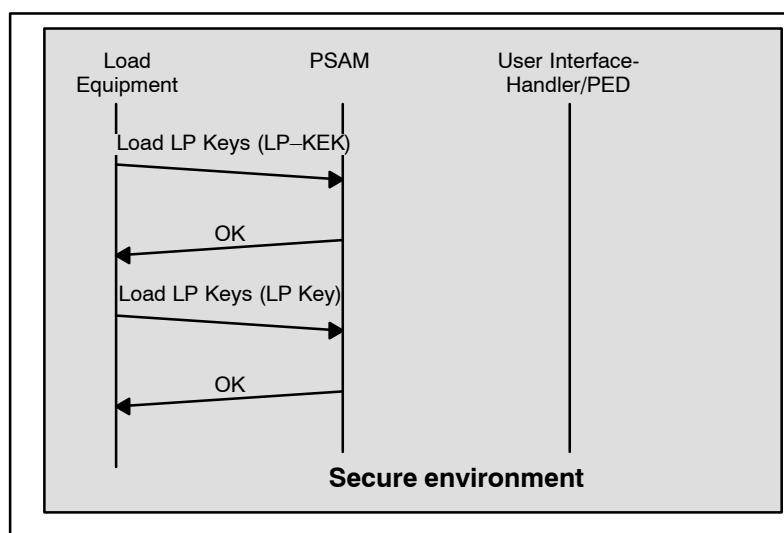
## P.6 Enciphered PIN Data

### P.6.1 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 P.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 P.1 and P.2.

LP-PPK is used to encipher the Enciphered PIN Data transferred to the PSAM in the *Local PIN Validation* command.

Table P.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 P.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 P.3.

Table P.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.

## P.6.2 Load LP Keys Command

The *Load LP Keys* command shall be used for load/exchange of LP-KEK(s) and LP-PPK(s).

P.6.2.1 A The *Load LP Key* command sent to the PSAM shall have the format shown in table 8.98.

The Response to the *Load LP Key* command will have the format shown in table 8.99.

### LP-KEK

When LP-KEK shall be exchanged the field LP-KEK-Data shall contain the new key value (LP-KEK<sub>NEW</sub>) enciphered by the previous value of the same key:

$$\text{LP-KEK-Data} = \text{DES3}(\text{LP-KEK}_{\text{PREVIOUS}})[\text{LP-KEK}_{\text{NEW}}]$$

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<sub>NEW</sub>) enciphered by the corresponding LP-KEK key (within the same key-chain):

LP-PPK-Data = DES3(LP-KEK)[LP-PPK <sub>NEW</sub> ]
--

### 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 <sub>NEW</sub> ) ['0000000000000000']}
---

or

Key Check Value = 3MSB{DES3(LP-PPK <sub>NEW</sub> )['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. 39: “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.

## P.6.3 Local PIN Validation command – Enciphered PIN

P.6.3.1 A When enciphered PIN is used, the *Local PIN Validation* command sent to the PSAM shall have the format shown in table 8.102.

A successful response to the *Local PIN Validation* command will have the format shown in table 8.104.

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. 39: “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 P.5.

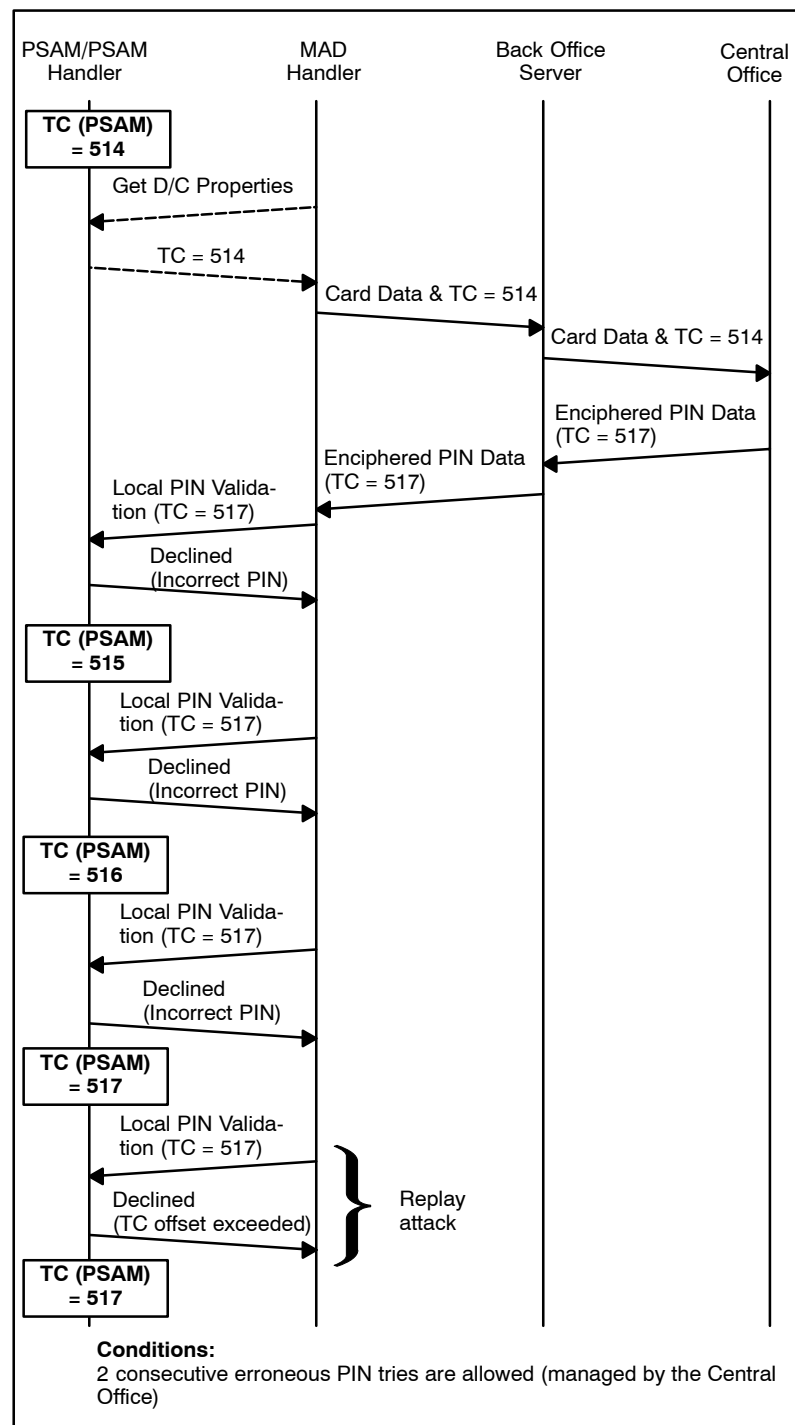
The allowed offset of 14 is designed to handle incorrect PIN entries without requiring a new (reference) PIN block from the entity generating the Enciphered PIN Block.

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 P.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 P.6.4 for more details.

The data element Transaction Counter will indicate the actual transaction sequence number.

## P.6.4 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 8.5.6 on page 8-28.

## P.6.5 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 8.6.6 on page 8-48.

## P.7 Limitations

### P.7.1 Enabling/Disabling of the Local PIN Validation functionality

Local PIN is only available when PBS 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.

### P.7.2 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

### P.7.3 PIN Range

P.7.3.1 A The number of PIN digits shall be in the range 4 – 12.

### P.7.4 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).

## P.8 Application Status Words (ASW1-ASW2)

For Application Status Words related to the Local PIN Validation, special ranges has been reserved:

Table P.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 (8.8.1)

Table P.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 8.122 – 8.125 on page 8–138.

## P.9 Message Codes

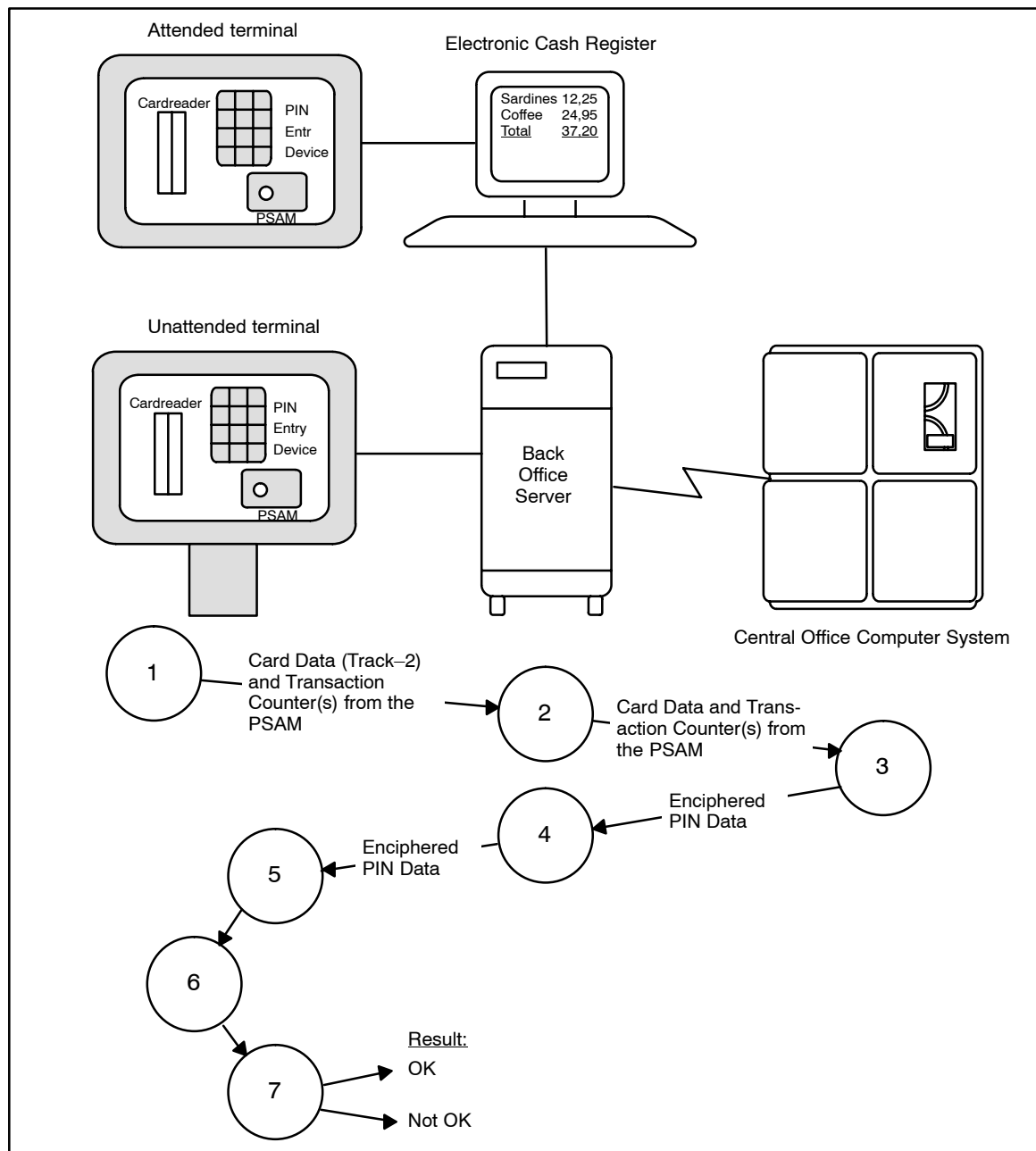
It is up to application owner to define relevant Message Codes (related to the ASW1–ASW2) to be displayed at the Cardholder Display.

## P.10 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 P.6.

Figure P.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, including 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

# Attachment Q. Status of Previous Transactions

## Q.1 Introduction

The PSAM offers a feature where the outside world (e.g. terminal or cash register system) can request the status of a previously performed transaction having financial impact.

This feature is described in the present attachment.

### Q.1.1 Duplicate Transaction Check performed by the PSAM

The PSAM also includes a function for automatic control of identical/duplicate transactions.

How this check is performed is described in section 7.20 “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 alternatively be disabled utilizing the same command.

The *Set Debit/Credit Properties* command is defined in section 8.5.7.

## Q.2 Functionality

### Q.2.1 General

#### 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 transactions is obtained by issuing a *Get Debit/Credit Properties* command as described in the next subclause.

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.

## Q.2.2 The Get Debit/Credit Properties Command

The *Get Debit/Credit Properties* command is 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 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 8.5.6 on page 8–28.

**NOTE:** Please note the limitations in usage given in section Q.4, “Limitations”.

## Q.3 Purpose of this Functionality

### Q.3.1 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.

### Q.3.2 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 Q.1.

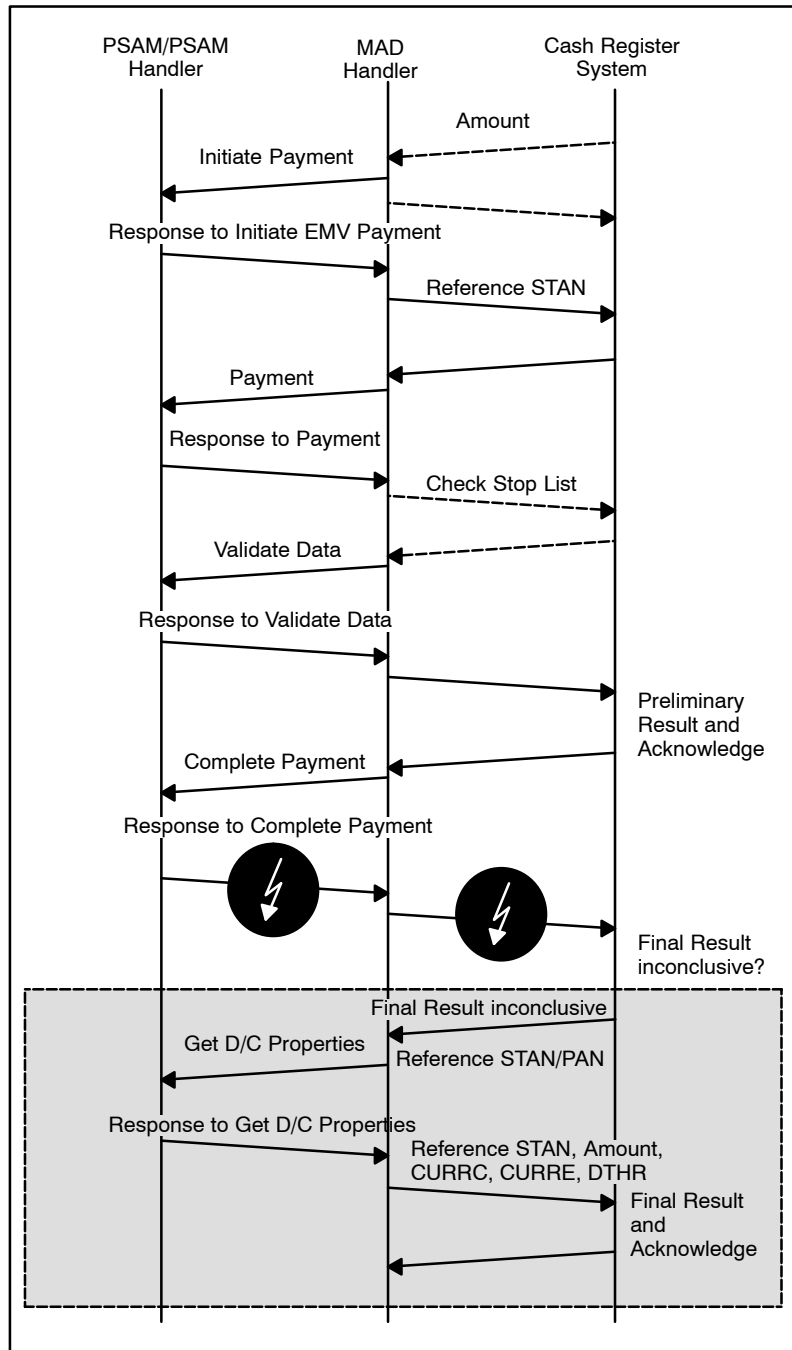


Figure Q.1 – Example of Command/Data Flow (Reference STAN)

### Q.3.3 PAN

If the Reference STAN is *not* known, the PAN may be used as search key instead.

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’.

## Q.4 Limitations

It is important to have the limitations described below in mind when designing systems using the status of the previous transactions.

### Q.4.1 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.

### Q.4.2 Transaction Types

Only transactions with financial impact are to be 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’)

### Q.4.3 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).

#### Q.4.4 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:** Until the PSAM has successfully completed 8 transactions and in so all 8 entries has been written, the PSAM may indicate a match, if the Reference STAN is used as search key with the value '00 00 00'. The value '00 00 00' is not a legal value for the Reference STAN.

#### Q.4.5 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.

# Attachment R. Implementation Conformance Statement (ICS)

## R.1 Introduction

The purpose of this attachment is to make it easier for the Terminal Supplier to fill in the mandatory Implementation Conformance Statement (ICS) required by EMVCo before any Level 2 test can be initiated.

This attachment will point out which parts of the ICS the Terminal Supplier has the responsibility to fill in and the actual values for the PSAM related parts of the ICS.

Note that it is up to the Terminal Supplier to retrieve the current version of the ICS from EMVCo ([www.emvco.com](http://www.emvco.com)). In case of any discrepancies between the current ICS from EMVCo and this attachment, please contact PBS. This attachment is based upon version 3.4 of the EMVCo ICS.

It is *highly* recommended to let PBS make a final review of the ICS before submitting it to EMVCo.

## R.2 Implementation Conformance Statement

Please read the instructions given at the end of the EMVCo ICS before further actions are made.

### R.2.1 Configurable Kernel

In case of configurable kernels, the column “Value supported” shall be filled in with “Yes / No” and “Yes” in the column “Configurable?” respectively.

In Part VI (Terminal Configurations), a column for each configuration has to be filled in.

Note, that the values stated in the tables below is applicable for a static kernel.

### R.2.2 Legend

The following tables comply with the “Implementation Conformance Statement (ICS) – Version 3.4 – Level 2 – EMV Application Kernel (Template for terminals compliant with EMV 4.x)”.

Where the symbol ☐ is indicated, it is up to the Terminal Supplier to insert the appropriate value. In case of doubt, do not hesitate to contact PBS.

EMVCo ICS		PBS Comments
<b>Part I – Application Provider Identification</b>		
EMV Registration Number:	<input type="text"/>	
Company Name:	<input type="text"/>	
Contact Name:	<input type="text"/>	
Address:	<input type="text"/>	
Telephone:	<input type="text"/>	
Fax Number:	<input type="text"/>	
Email Address:	<input type="text"/>	
I hereby declare that the following referenced product currently is and will remain in compliance with the following referenced EMV specification for all mandatory and supported optional requirements unless noted as non-compliant on the attached sheets.		
Signature and Date:	<input type="text"/>	
ICS Identifier: <i>For administrative use only</i>	<input type="text"/>	

EMVCo ICS	PBS Comments
<p><b>Kernel Type</b></p> <p><i>Please use the drop-down box below to select the kernel type which applies to this submission (session):<sup>1</sup></i></p> <ul style="list-style-type: none"> <li>– Static kernel</li> <li>– Static W/ PIN Pad Process</li> <li>– Configurable – New Kernel</li> <li>– Configurable – Additional Configurations</li> </ul> <p><input type="text"/></p> <p><i>If you have selected “Configurable – Additional Configurations”, then please provide the associated information below:</i></p> <p>Baseline Approval Number; and/or Baseline ICS ID:</p> <p><input type="text"/></p>	<p>Chose “Configurable – New kernel” or “Configurable – Additional Configurations” if more than one configuration is going to be tested. In case of “Configurable kernel”, the column “Configurable?” in the tables shall be filled in for every row.</p>

EMVCo ICS	PBS Comments
<p><b>ICS</b></p> <p><i>Select New or Replacement</i></p> <p><i>If Replacement (due to a revision of options, descriptions, etc.), please provide existing ICS ID: (Leave blank for new kernel)</i></p> <p><input type="text"/></p>	

<sup>1</sup> At this time, the MCK and PIN pad process is limited to 1 configuration.

EMVCo ICS		PBS Comments
<b>Part IIa – EMV Application Kernel Identification</b>		
Device/terminal “Marketing name” within which the Application Kernel was tested	☞	
Application Kernel Name and Version	☞	
EMV Kernel Operating System or Platform:	PBS PSAM ‘8111’ V. 005X	Example, to be obtained from PBS
Operating System or Platform Version:	☞	
<p>The application kernel may be contained within a single location, module, or library in which case the entries above must be complete. However, when the application kernel is split across several subcomponents (ECR, PIN Pad, server, etc.) these must be fully described below:</p> <p><u>Product Name Type of Component Software Name Software Ver.</u></p> <p>☞</p>		
Device reference where each subcomponents resides:		
Subcomponent(s) operating system if different from EMV Kernel operating system. All entries must identify product name, OS name and version.		
IFM (Level 1) Approval Reference <sup>2</sup>	☞	

- <sup>2</sup> When supporting the PIN Change Process the IFM Approval Reference may vary for some PIN Pads, if so these references must be identified in section 11b.

EMVCo ICS	PBS Comments
<b>Part IIb – Additional PIN Pad Identification</b>	Normally not filled
This section applies to the PIN Pad Change process only	

EMVCo ICS		PBS Comments
<b>Part III – Terminal Resident Data Objects</b>		
	Value	Configurable?
Terminal Type	☞	☞
The following data elements are for testing purposes only. Even though the data object are variable, please provide what values exist in terminal to make testing possible.		If configurable, all Terminal Types shall be listed
	Value	
Terminal Country Code:	0208, Denmark	
Application Version Number:	☞	
Terminal Currency Code:	0208, DKK	

EMVCo ICS		PBS Comments
<b>Part IV – EMV Specifications</b>		
EMV Specification Date & Version	EMV 2000 Integrated Circuit Card Specification for Payment Systems version 4.0 December 2000	

**NOTE:** When completing this section, please enter the hexadecimal value equivalent to the Terminal Capabilities and Additional Terminal Capabilities. This to ensure the application coding matches the capabilities identified.

EMVCo ICS		PBS Comments
<b>Part V – Terminal Details</b>		

EMVCo ICS			PBS Comments
<b>Terminal capabilities</b>		<b>Value Supported</b>	<b>Configurable?</b>
<b>Card Data Input Capability</b>		XX ☐	Insert hexadecimal value
O	Manual Key Entry	No	<i>Not</i> supported by PSAM
O	Magnetic Stripe	Yes	Supported by PSAM
M	ICC with contacts	<b>Yes</b>	<b>No</b> Supported by PSAM
<b>CVM Capability</b>		F8	Insert hexadecimal value
O	Plaintext PIN for ICC Verification	Yes	Supported by PSAM
O	Enciphered PIN for online Verification	Yes	Supported by PSAM
O	Signature (paper)	Yes	Supported by PSAM
O	Enciphered PIN for offline Verification	Yes	Supported by PSAM
O	No CVM Required	Yes	Supported by PSAM
<b>Security Capability</b>		XX ☐	Insert hexadecimal value
C	Static Data Authentication ( <b>Mandatory</b> for offline capable terminals and terminals supporting DDA)	Yes	No Supported by PSAM
O	Dynamic Data Authentication	Yes	No Supported by PSAM
O	Card Capture	☐	
O	Combined Dynamic Data Authentication / Application Cryptogram Generation	Yes	No Supported by PSAM




EMVCo ICS		PBS Comments	
Additional Terminal capabilities		Value Supported	Configurable?
<b>Transaction Type Capability</b> At least one of the following transaction types must be supported:		XX 00 ☞	Insert hexadecimal value
O	Cash	Yes <sup>1)</sup>	Supported by PSAM
O	Goods	Yes <sup>1)</sup>	Supported by PSAM
O	Services	Yes <sup>1)</sup>	Supported by PSAM
O	Cash back	(No)	Currently not supported
O	Inquiry	No	
O	Transfer	No	
O	Payment	No	
O	Administrative	No	
O	Cash Deposit	No	
<b>Terminal Data Input Capability</b>		XX ☞	Insert hexadecimal value
O	Does terminal have a keypad? (if keypad is supported the terminal shall support one or more of the following key types)	☞	
C	Numeric Keys	☞	
C	Alphabetic and Special Character Keys	☞	
C	Command Keys	☞	
C	Function Keys	☞	
<b>Legend:</b>			
<sup>1)</sup> = Either Goods & Services or Cash. In case of Quasi–Cash contact PBS.			

EMVCo ICS			PBS Comments	
<b>Terminal Data Output Capability</b>				
C	Print, Attendant ( <b>Mandatory</b> for terminals supporting signature)	<input type="checkbox"/> <sup>1)</sup>		
O	Print, Cardholder	<input type="checkbox"/> <sup>1)</sup>		
C	Display, Attendant ( <b>Mandatory</b> for Attended terminals)	<input type="checkbox"/> <sup>1)</sup>		
O	Display, Cardholder	<input type="checkbox"/> <sup>1)</sup>		
O	Code Table 10	<input type="checkbox"/>		
O	Code Table 9	<input type="checkbox"/>		
O	Code Table 8	<input type="checkbox"/>		
O	Code Table 7	<input type="checkbox"/>		
O	Code Table 6	<input type="checkbox"/>		
O	Code Table 5	<input type="checkbox"/>		
O	Code Table 4	<input type="checkbox"/>		
O	Code Table 3	<input type="checkbox"/>		
O	Code Table 2	<input type="checkbox"/>		
O	Code Table 1	Yes		
<b>Legend:</b>				
<p><sup>1)</sup> = If the terminal is attended (Terminal Type = 'x1', 'x2', or 'x3') and there is only one printer, the 'Print, attendant' line shall be set to 'Yes' and the 'Print, cardholder' line shall be set to 'No'.</p> <p>If the terminal is attended and there is only one display, the 'Display, attendant' line shall be set to 'Yes' and the 'Display, cardholder' line shall be set to 'No'.</p> <p>If the terminal is unattended (Terminal Type = 'x4', 'x5', or 'x6'), the 'Print, attendant' and 'Display, attendant' line shall be set to 'No'.</p>				

EMVCo ICS			PBS Comments	
Application Selection		Value Supported	Configurable?	
O	Support PSE selection Method	<input type="checkbox"/>		
O	Support Cardholder Confirmation	Yes		
O	Does Terminal have a preferred order of displaying applications?	<input type="checkbox"/>		Normally not supported
M	Does terminal perform partial AID selection?	Yes	No	
O	Does the terminal have multi language support?	<input type="checkbox"/>		
M	Does the terminal support the Common Character Set as defined in Annex B Table 20 Book 4	Yes	No	

EMVCo ICS			PBS Comments	
Data Authentication		Value Supported	Configurable?	
C	What is the maximum supported Certificate Authority Public Key Size? ( <b>Mandatory</b> for terminals supporting Data Authentication with minimal support of 248 bytes)	248	No	
C	What exponent does the terminal support? ( <b>Mandatory</b> for terminals supporting Data Authentication, 3 and $2^{16}+1$ )	3 and $2^{16}+1$	No	
O	During data authentication does the terminal check validity for revocation of Issuer Public Key Certificate	No	No	
C	Does the terminal contain a default DDOL? ( <b>Mandatory</b> for terminals supporting DDA)	Yes	No	
O	Is operation action required when loading of CA Public Key fails	No	No	
O	CA Public Key verified with CA Public Key Check Sum? If no, provide a description of the method used to validate the CA Public Key when loaded in the Comments and Explanations section.	No	No	Controlled by proprietary MAC computation.

EMVCo ICS			PBS Comments	
Cardholder Verification Method		Value Supported	Configurable?	
O	Terminal supports bypass PIN Entry	No	No	
O	Terminal supports Get Data for PIN Try Counter	Yes	No	
M	Terminal supports Fail CVM	<b>Yes</b>	<b>No</b>	
O	Are amounts known before CVM processing?	Yes	No	

EMVCo ICS			PBS Comments	
Terminal Risk Management		Value Supported	Configurable?	
C	Floor limit checking ( <b>Mandatory</b> for offline only terminals and offline terminals with online capability)	Yes	No	
C	Random Transaction Selection ( <b>Mandatory</b> for offline only terminals and offline terminals with online capability)	Yes	No	
C	Velocity Checking ( <b>Mandatory</b> for offline only terminals and offline terminals with online capability)	Yes	No	
O	Transaction Log	No	No	
O	Exception File			Stop List
O	Performance of Terminal Risk Management based on AIP setting?	No	Yes	

EMVCo ICS			PBS Comments	
Terminal Action Analysis		Value Supported	Configurable?	
O	Does the terminal support the Terminal Action Codes	Yes	No	
Offline Only terminals <b>shall</b> support one of the following:				
C	Does Offline Only Terminal process Default Action Codes prior to First Generate AC	Yes	No	
C	Does Offline Only Terminal process Default Action Codes after First Generate AC	No	No	

EMVCo ICS			PBS Comments	
Completion Processing		Value Supported	Configurable?	
O	Transaction Forced Online Capability	<input type="checkbox"/>		Supported by PSAM
O	Transaction Forced Acceptance Capability	No	No	
O	Does terminal Support Advices	No	No	Separate from an Authorisation request or a clearing message
C	Does the terminal support Issuer initiated Voice Referrals?	No	No	
C	Does the terminal support Batch Data Capture? ( <b>Mandatory</b> for Offline Capable Terminals)	Yes	No	
O	Does the terminal support Online Data Capture	No	No	
O	Does the terminal support a Default TDOL	Yes	No	

EMVCo ICS			PBS Comments	
Exception Handling		Value Supported	Configurable?	
C	What is the POS Entry Mode value when IC cannot be read and the transaction falls back using Magstripe ( <b>Mandatory</b> for attended terminals)	'XX7XXX' in host message, '80' in issuer message		

EMVCo ICS			PBS Comments	
Miscellaneous		Value Supported	Configurable?	
O	Is the terminal equipped with a PIN Pad?	<input type="checkbox"/>		
O	Is the amount and PIN entered at the same keypad?	<input type="checkbox"/>		
O	Is the ICC/Magstripe Reader combined?	<input type="checkbox"/>		
O	If Combined ICC/Magstripe Reader is supported, is Magstripe read first?	<input type="checkbox"/>		
O	Does the terminal support account type selection?	No	No	Not supported currently

EMVCo ICS	PBS Comments
<p><b>Comments and Explanations:</b></p> <p><u>Data Authentication, Check Sum:</u></p> <p>MAC validation assures that the CA Public Key is authentic when loaded in a Secure Modul in the terminal (PSAM). Only the host is able to compute the correct MAC.</p>	

EMVCo ICS			PBS Comments
<b>Part VI – Terminal Configurations</b>			
ICS Feature	Configura- tion 1	Configura- tion 2	
To be continued			PSAM values retrieved from previous parts. A column shall be filled in for each configura- tion.

# Attachment S. Terminals with Combined Cardholder and Merchant Interface

## S.1 Introduction

An attended terminal may be designed as a Single Unit Terminal 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.

## S.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 hand over temporary 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:

- "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 table S.1.



Table S.1 – Transaction Flow

Step	Operator	Functions
1	Merchant	<u>Setup transaction conditions</u> <ul style="list-style-type: none"> <li>– Select Transaction Type (Purchase/Refund)</li> <li>– Amount Entry</li> <li>– Select 'Forced Signature' (if relevant)</li> <li>– Select Fallback (if using the ICC has failed)</li> <li>– Select 'Forced Offline' (if relevant/implemented)</li> </ul>
2	Cardholder	<u>Cardholder Card entry, PIN entry and amount acceptance</u> <ul style="list-style-type: none"> <li>– Card Entry (Insert or swipe)</li> <li>– Application Selection</li> <li>– PIN Entry</li> <li>– Amount Approval</li> <li>– "Wait" while (online) processing is completed</li> <li>– Display result: <ul style="list-style-type: none"> <li>– PIN/No CVM: Display &lt;final result&gt; to the Cardholder and "Afler Terminal"</li> <li>– Signature: Display "Afler Terminal"</li> </ul> </li> </ul>
3	Merchant	<u>Merchant Transaction completion</u> <ul style="list-style-type: none"> <li>– The Merchant continues the flow by activating a 'specific key or function' (implementation dependent).</li> <li>– Print receipt(s)</li> <li>– Accept signature (if required)</li> <li>– Print additional receipt(s).</li> <li>– The &lt;final result&gt; is displayed to the Merchant.</li> </ul>

### S.3 Examples

Figures S.1 to S.4 on the following pages depict examples of the general message flow during different types of transactions.

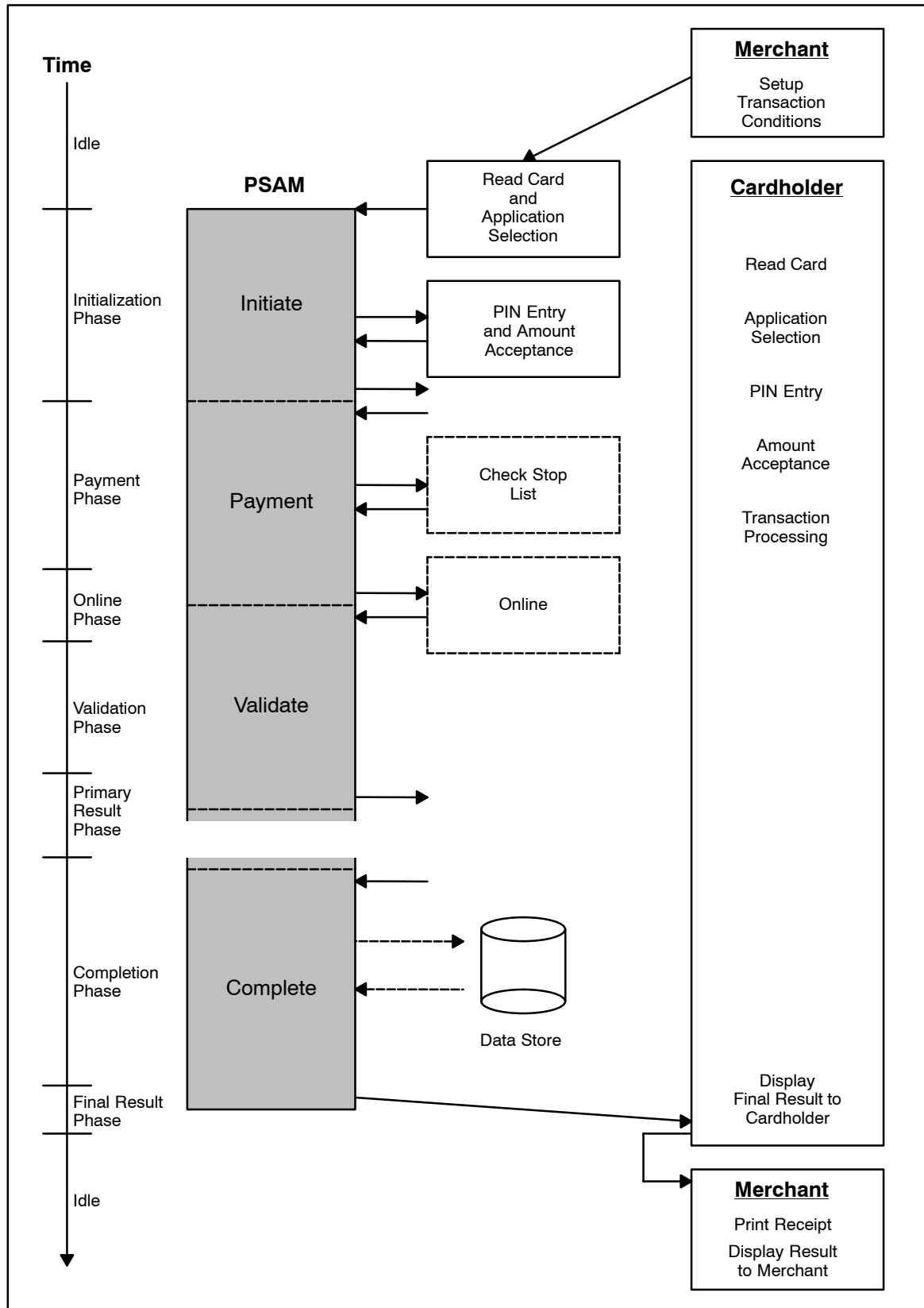


Figure S.1 – PIN Transaction

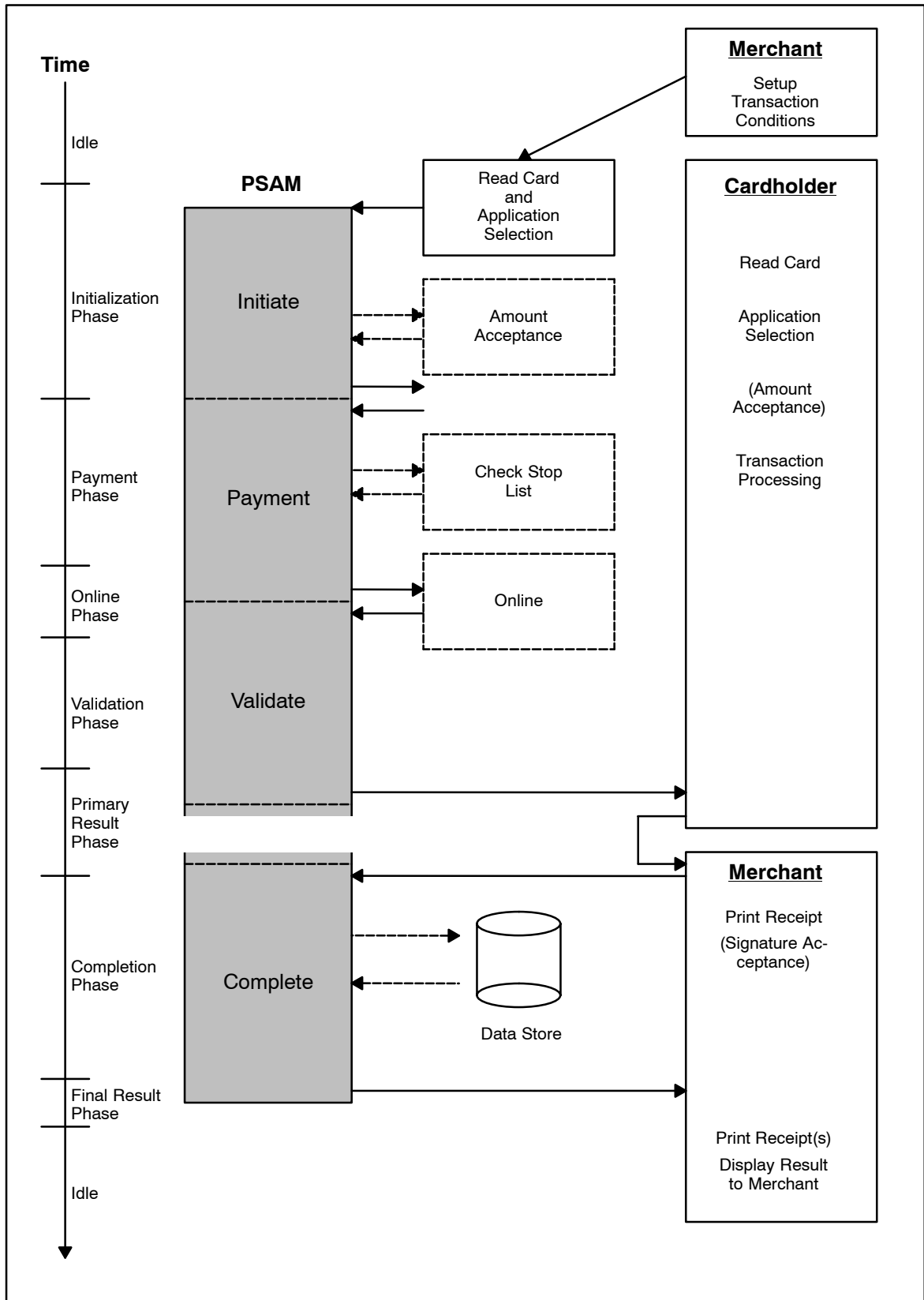


Figure S.2 – Signature Transaction

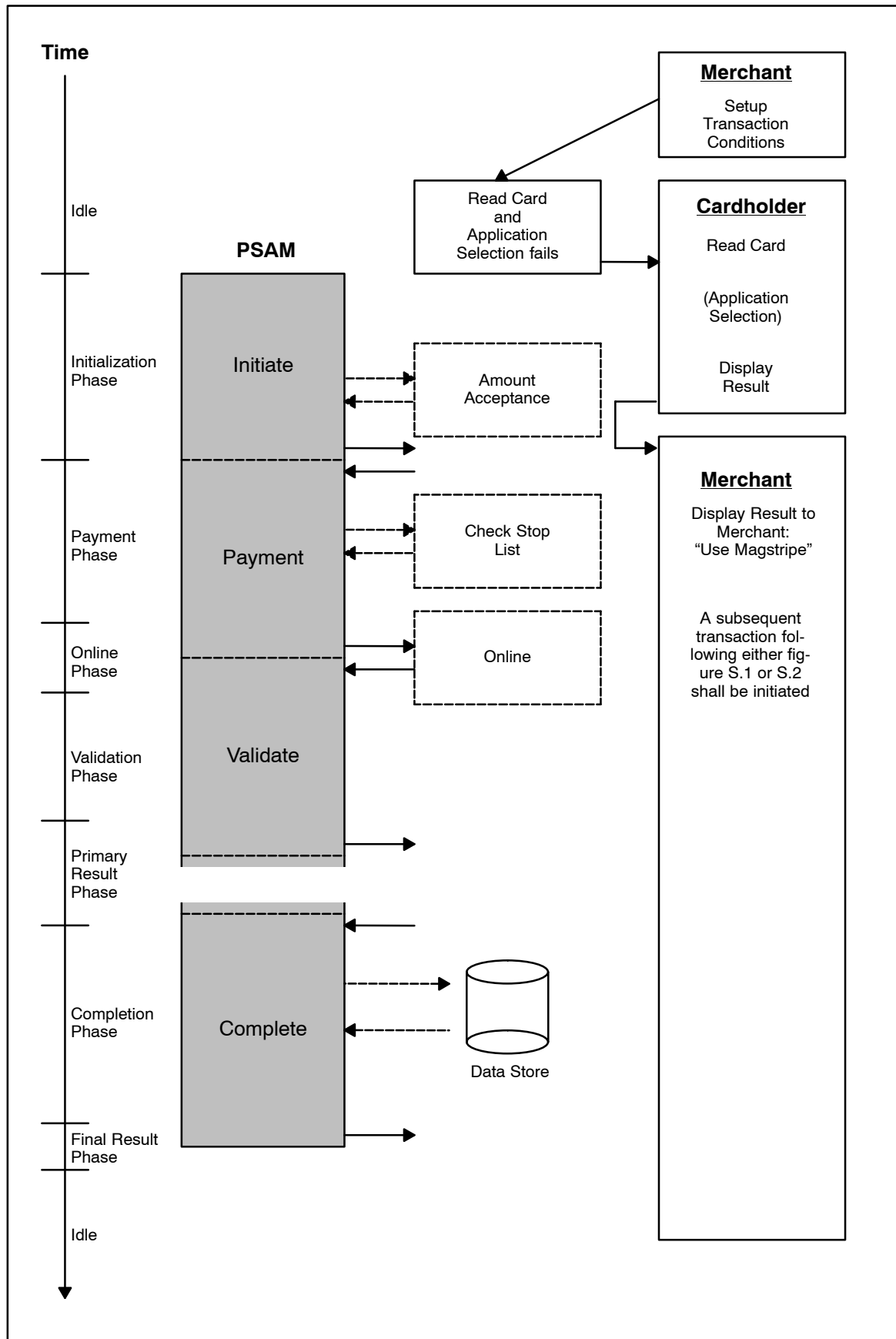


Figure S.3 – Fallback (Noticed before Application Selection is Completed)

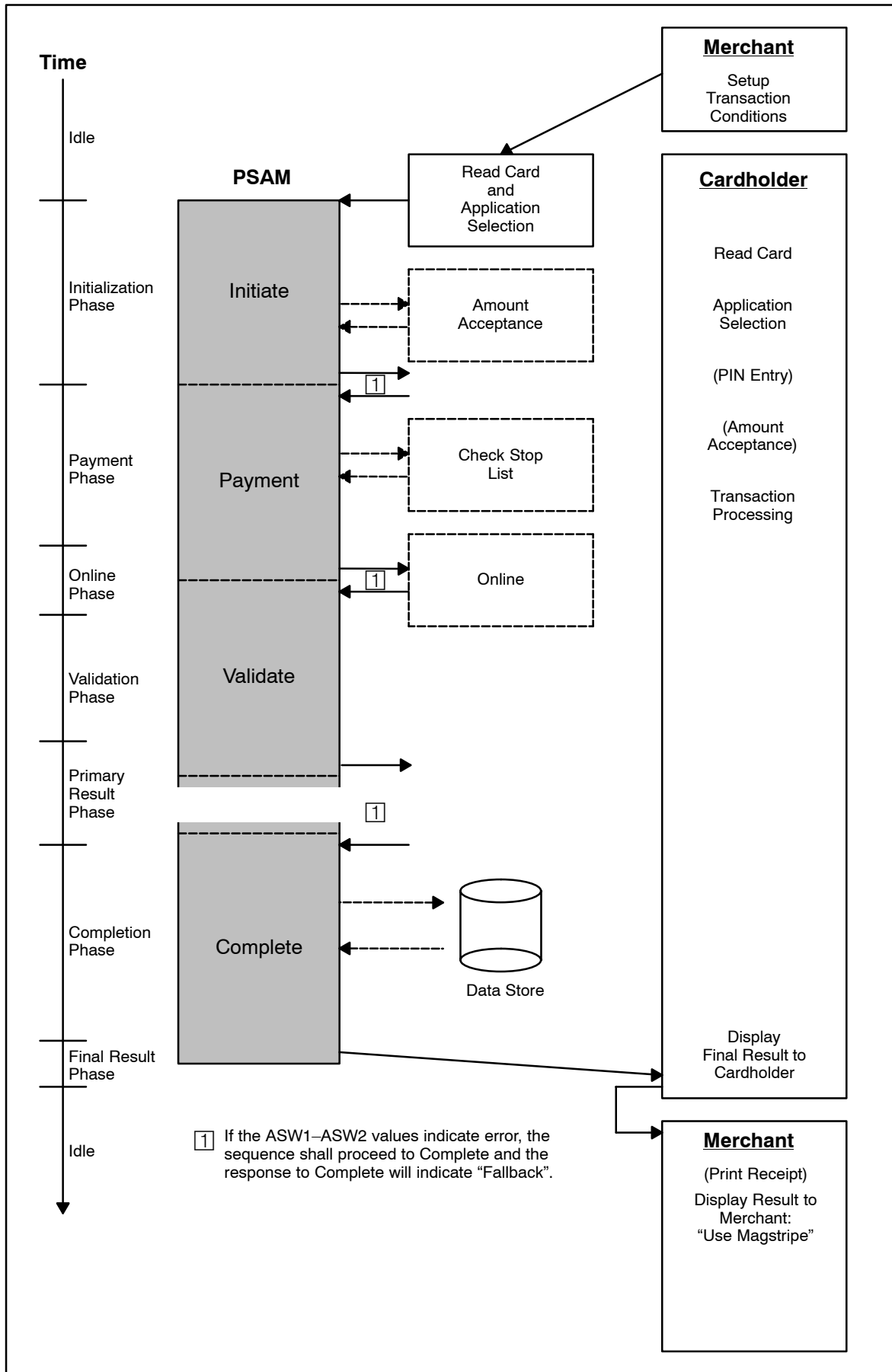


Figure S.4 – Fallback (Noticed after Application Selection is Completed)

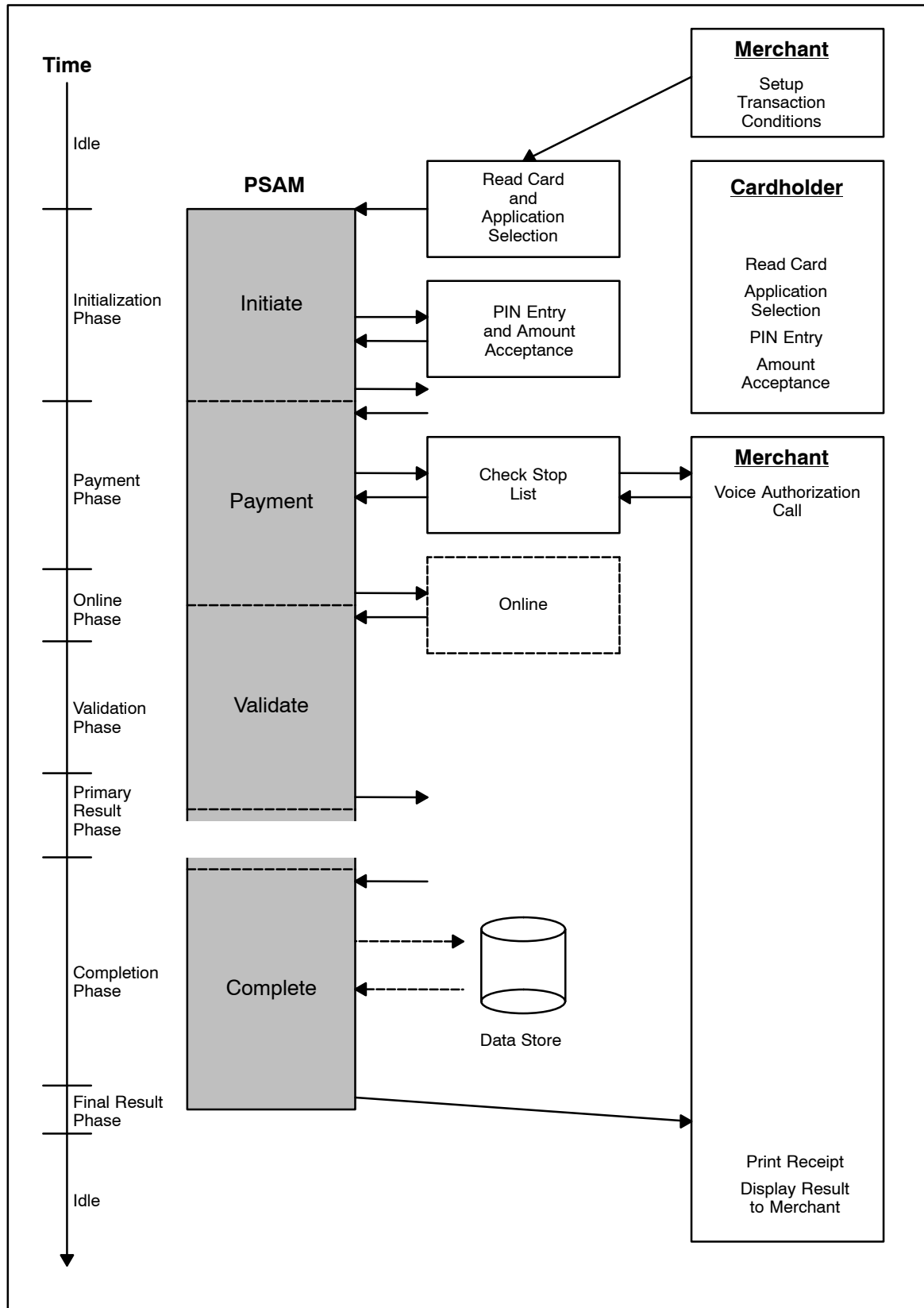


Figure S.5 – PIN Transaction – Forced Offline

**NOTE:** The Voice Authorization Call is based upon the PAN returned from the PSAM in the *Check Stop List* command.

# Attachment Z. Problem Reporting

If any kind of problem or error is detected in this specification, PBS A/S would appreciate a notification hereof.

Please fill in a copy of the Problem Report shown on the next page with an exhaustive description of the problem, and mail or fax it to this address:

PBS A/S

Lautrupbjerg 10  
DK–2750 Ballerup  
DENMARK

Tel.: +45 4468 4468, Fax : +45 4486 0930

or alternatively to:

[pe.862@pbs.dk](mailto:pe.862@pbs.dk)

<b>Problem Report</b>		No. (PBS use):	
Reported by:		Date:	
Document Name: <b>Technical Reference Guide – Open Terminal Requirement Specification</b>			
Document Version: <b>2.5</b>	Page:	Placing:	
Problem Type (circle): Superfluous      Missing      Wrong      Inconsistent      Unclear			
Problem Description:			
Problem Consequence:			
Suggested Solution (if any):			
<u>Reserved PBS</u>		Status: Open Closed	
Priority:      Immediate    Important    Later    Rejected			
Action:			
Responsible Designer:		Completed Date:	



# Index

Page references in **bold** type refer to either figures or tables.

## A

- A–requirements, Definition, 3–6
- AAC, 5–36, F–84
  - Abbreviations, 3–1
- AAR, Abbreviations, 3–1
- Accelerated PIN Entry, 6–54, I–2
  - Best Practice, 7–8
  - Gavekort, I–2
- Accelerated PIN Entry Vs. Original Flow, **6–55**
- Access to the inside of the terminal, H–6
- Account Type, 8–38, 8–52, 8–66, **9–2**
  - Definition, 9–2
- Account type, R–9
- Accuracy, Real time clock, 10–5
- Accurate Amount, 9–4
  - Get Amount 3, 8–85
- Acquirer, 4–9
- Acquirer Identifier, 6–53
- Action Code, 6–48, 6–73, 6–93, 6–121, 6–129, 6–150, 6–153, 8–43, L–2, L–3
  - Applicable values, **F–77**
  - Definition, 9–2
  - Field 39, F–76
  - National Use, **6–153**
  - Position 1, 6–153, **F–76**
  - Position 2, 6–153, **F–76**
- Action CodePRINT, 8–47
- Add Addendum Record
  - Command, 6–118, 6–119
  - Description, 8–24
- Addendum, 9–4
- Addendum Record, 6–119, 8–24, F–56, F–74
  - Command flow, **6–120**
  - Definition, 9–2
  - Description, 6–118
  - Field 72, F–87
- Addendum Status, 6–119, 8–24
- Adding records to File–5, L–2
- Addition of Surcharges and Fees, Best Practice, 7–16
- Additional AID Info, Get Debit/Credit Properties, 8–30
- Additional Data – National, Field 47, F–83
- Additional Fees, Receipt, 1–16, G–19
- Additional Info, 8–28, 8–32
- Additional MSC Info, Get Debit/Credit Properties, 8–30, 8–31
- Additional PSAM Info, 9–18
  - Get Debit/Credit Properties, 8–30
- Additional Response Data, Field 44, F–80
- Additional Terminal Capabilities, 6–53, 6–123, 8–19, 8–21
  - Field 46, F–82
- Additional Terminal capabilities, ICS, R–5
- Adjustment, F–64
- Administrative Advice, 6–124
  - Definition, **F–56**
- Administrative Transactions, **6–121**
  - Description, 6–121
- Advice Enclosing, Description, 6–123, 6–131
- Advice Forwarding, 6–150
  - Description, 6–123
- Advice Handling, **6–125**
- Advice Request Flag
  - APACS Header, F–6
  - Coding, F–15
  - Description, 6–139
- Advice Transfer, 4–21, **6–121**, 6–129, **6–130**, 6–150
  - Definition, F–60
  - Description, 6–123, 6–128
  - Gift Voucher, I–7
  - Re–send, 6–150
- Advice Window Size
  - APACS Header, F–6
  - Coding, F–15
  - Description, 6–127
- Advice Window Size (Examples), **6–132**
- Advices Enclosing, 6–150
- AED, Receipt text, G–7
- AID, 5–25, 5–29, 6–41, 8–36, 8–38, 8–65, 8–67
  - Abbreviations, 3–1
  - Definition, 9–3
  - Exact match, 9–4
  - Get Debit/Credit Properties, 8–30
  - Partial match, 9–4
  - Receipt text, G–7
  - Selection Record, **5–25**

- Selection Table, 5–25
- AIP, F–84
- Airlines, F–75, F–87
- ALG<sub>VLP</sub>, Definition, 9–3
- Alpha–characters, 5–15, 10–11
- Amount, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66
  - Definition, 9–3
  - Get Debit/Credit Properties, 8–30
  - Local PIN, 8–88, 8–90
- Amount Authorized, F–84
- Amount Confirm Indicator, 6–155
- Amount Other
  - Get Amount 2, 8–83
  - Get Amount 3, 8–85
- Amount Request
  - Definition, 9–3
  - Get Amount 3, 8–84
  - Service Pack No. 2, 11–5
- Amount Status
  - Definition, 9–4
  - Get Amount 3, 8–85
  - Service Pack No. 2, 11–5
- Amount, Other, 6–43, 6–69, 6–89, 6–104, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66, F–84
  - Definition, 9–3
- Answer–to–Reset, 5–18, 9–17
- APACS, 6–145, 6–153, 9–16, F–6
  - Example, F–11
- APACS Header, F–6, F–8
- APACS MAC Key Version
  - APACS Header, F–6
  - Coding, F–14
- APACS Message Header, Description, F–4
- APACS Message Types, F–4
- APACS60, F–2
- APDU, 6–134, 8–4
- APE
  - Abbreviations, 3–1
  - Accelerated PIN Entry, 6–54
  - Best Practice, 7–9
- Application Cryptogram, F–84
- Application Effective Date, 6–43
- Application Identifier, Definition, 9–3
- Application Interchange Profile, F–84
- Application Label, 5–30, 6–51
  - Definition, 9–4
- Application layer, F–2
- Application Layers, F–3
- Application Preferred Name, 5–30
- Application Priority Indicator, 5–32
- Application Selection, 4–18, 5–31
  - Best Practice, 7–4
  - Description, 5–22
  - ICS, R–6
  - Introduction, 4–18
- Application Selection Indicator, 5–25
  - Definition, 9–4
- Application Status Words, 5–36, 6–44, 6–152, 8–4, 8–93
  - Field 46, F–82
  - Receipt, G–11
- Application Transaction Counter, F–84
- Applications Effective Date, G–7
- Applications Transaction Counter, G–7
- Approval Code, 6–45, 6–71, 6–72, 6–91, 7–7, 8–47, 8–72, G–8
  - Definition, 9–4
  - Service Packs, 11–4
- Approval tone, 10–10
- Approved/Successful Transactions, Previous Transaction Status, Q–5
- ARC, 8–47
  - Receipt text, G–8
- ARQC, F–84
  - Abbreviations, 3–1
- ASI, 5–25
  - Definition, 9–4
  - Get Debit/Credit Properties, 8–30
- ASN.1, F–5
  - Abbreviations, 3–1
- ASW1 ASW2, 6–143, 6–153, G–10
  - Abbreviations, 3–1
  - Approved/Successful, 8–97
  - Approved/Successful – Action Requested, 8–97
  - Converted to Message Codes, 8–95
  - Declined, 8–105
  - Declined – Pick up, 8–107
  - Error – Action Requested, 8–101
  - Failed – No Retry, 8–110
  - Failed – Retry, 8–108
  - Range, 8–96
  - TAPA defined, 8–92
- ASW1–ASW2 Coding, 8–92
- ASW1–ASW2 grouping, 8–93
- ASW1–ASW2 Ranges, Local PIN Validation, P–11
- ASWs, Handling, 6–144
- ATC, 6–46, 6–47, 8–41, 8–69, F–84
  - Receipt text, G–7

ATM, E-1

ATR, 10-18, 10-19  
 Abbreviations, 3-1  
 ICC, 5-10  
 PSAM, 5-18  
 PSAM values, **5-18**

Attended, F-69

Attributes for APACS 60 Messages, Notation, 3-5

Audio Indicator, Description, 5-16, 10-10

Audio indicator, 10-11

Auditory environment, 10-1

AUT KODE, Receipt text, G-8

Authorisation Code, 6-45, 6-71, 6-72, 6-91, 8-72

Authorisation Response Code, F-80, F-84, G-8

Authorization, Terms, 3-3

Authorization Advice, 6-152  
 Definition, **F-26**

Authorization Request, Definition, **F-20**

Authorization Response Code, Service Packs, 11-4

Authorized Person, H-1

Automated Dispensing Machines, E-1, E-2

Automatic Advice Transfer if no Customers being Serviced, Best Practice, 7-17

Availability, Previous Transaction Status, Q-5

## B

B-requirements, Definition, 3-6

Backup message, F-75

Balance inquiry, Gavekort, I-5

Bar code, Gavekort, I-14

Basic Regulations, 4-5

Batch Number, 6-45, 6-119, 6-137, 8-24, 8-40, 8-54, 8-60, 8-68, N-2, N-3  
 Definition, 9-4  
 Requirements, 6-137

Battery back-up, 10-5

Baud rate, 5-19

Bell-connector, 10-8

Bellcore attack, 5-12

BER-TLV, F-5

Best Practice, 7-1

Bibliography, 3-11

Binary, Notation, 3-4

Bit Numbering, Notation, 3-4

Black list, F-75

Build date, 6-2

Business Call, 6-32  
 Terms, 3-3

Business Calls, 6-39, 6-67, **G-5**, G-25, K-1  
 Description, 6-14  
 Gavekort, **I-2**

Business Calls Vs. Amount, **6-21**

Business Environment – Characteristics, Receipt, **G-29**

Business Registration Number, Definition, 9-12

Business Requirements, 4-6  
 Local PIN, P-1

Buying with a Gavekort, Gavekort, I-5

BWI, **5-19**

## C

C-requirements, Definition, 3-6

CA, Abbreviations, 3-1

CA Public Key, ICS, R-7

CAD, Abbreviations, 3-1

CAD Management/Service Quality Data, Field 46, F-11, **F-81**

CAD output capability, **F-66**

CAD security capability, **F-65**

Call numbers, 7-17

CAM, Abbreviations, 3-1

Cancel, 10-15

Cancel button, 6-151, 6-152, 6-155

Cancelled, G-10

Candidate List, 5-29, 5-30, 5-32, 5-38, 5-40  
 Best Practice, 7-4  
 Number of entries, 5-29

Capture, 4-20, 6-17, 6-118, K-1

Car Rental, 4-8, F-75, F-87

Carbon Copy, Receipt, G-17, G-18

Card Action Analysis, 6-44

Card Capture, ICS, R-4

Card Data, 8-75, H-1  
 Definition, 9-5

Card Data Entry, G-24

Card Data Input Capability, ICS, R-4

Card Data Source, 6-41, 6-68, 6-88, 6-103, 8-36, 8-38, 8-50, 8-52, 8-58, 8-64, 8-66  
 Best Practice, 7-3

- Definition, 9–5
- Card Declined Transactions, Definition, 6–151
- Card Handler, Description, 5–7
- Card inserted correctly?
  - Best Practice, 7–3
  - Merchant Display, 5–35
- Card Issuer, 4–10
- Card Name, 5–30, 5–35, 6–43, 6–70, 6–75, 6–95, 6–109, 8–37, 8–39, 8–51, 8–53, 8–59, 8–65, 8–67, **F–81**, G–6
  - Definition, 9–5
  - for printing, F–80
  - Get Debit/Credit Properties, 8–30
- Card Reader error, F–12
- Card Reconciliation Counter ID, F–80, N–2
- Card Reconciliation Counter Name, F–80, N–2
- Card Related Transactions, 6–39
- Card Risk Management, 9–21
- Card Selection, 4–18, 5–8
- Card selection table, 4–17
- Card Sequence Number, Definition, 9–5
- Card Serial No., **A–2**, **A–3**
- Card Service Info, 5–35
  - Coding, **9–5**
  - Definition, 9–5
  - Get Debit/Credit Properties, 8–30, 8–31
- Card slot, 10–7
- Cardholder, 4–9
- Cardholder Activated Terminals, Description, E–1
- Cardholder Confirmation, ICS, R–6
- Cardholder Display, 6–31, 6–33, 8–93, 8–94, 10–9
  - Description, 5–14
  - Terms, 3–3
- Cardholder Initiated Actions, Definition, 6–151
- Cardholder Key Pad, Description, 5–14
- Cardholder Keyboard, Description, 10–11
- Cardholder Verification, 6–41
- Cardholder Verification Method, 6–25, 8–94
  - Best Practice, 7–5
  - ICS, R–7
- Cash, **7–24**, 9–23, F–64
  - ICS, R–5
- Cash Advance Terminals, 4–8
- Cash Register, 10–27, 10–28
  - Logging, G–25
- Cash register, 7–14
  - Best Practice, 7–13
- Cash/Quasi–Cash – Applicable Business Calls, **7–20**
- Cash/Quasi–cash Terminals, **7–20**
  - Best Practice, 7–20
- Cashback, 6–19, 6–24, 6–43, 6–69, 6–89, 6–104, 9–3, K–1, N–8
  - Best Practice, 7–15
  - ICS, R–5
  - Receipt, G–19
  - Token, 6–28
- Cashback Amount, Best Practice, 7–15
- CAT, 4–8, 5–1, 5–7, 6–121, 6–124, 10–6, E–1, G–2
  - Abbreviations, 3–1
  - Level 1, E–2, F–69
  - Level 2, E–2, F–68, F–69
  - Level 3, E–2, F–68, F–69
  - Level 4, E–2
  - Levels, E–1
- CDA, 4–17, 4–25
  - Abbreviations, 3–1
- CDOL1, 6–44, 9–11
- CDOL2, 6–46, 9–11
- Central European Time, 6–136
- CEP, 4–1
  - Abbreviations, 3–1
- Certificate Authority Public Key Size, ICS, R–7
- Certification, 4–26
  - Description, D–1
- CET, 6–136
- CHAP, F–3
- Character height, 10–9
- Check digit 1, **A–2**, **A–3**
- Check digit 2, **A–2**, **A–3**
- Check Stop List, 6–45
  - Description, 8–71
- Check Stop List command, 6–45, 6–71
- Check Value, Handling, **6–127**
- Check value, 6–121, 6–126, L–2, L–3
- Choice of Business Call, Best Practice, 7–2
- Circuit Design, Description, 10–17
- CLA, Abbreviations, 3–2
- Clean Up, Complete Payment command, 5–4
- Clear, 10–15
- Climatic environments, 10–1
- CLK pin, 10–19
- Clock, Real–time, 10–5

- Clock Frequency, Best Practice, 7–9
- Clock frequency, 10–18, 10–19
- Clock Synchronization, **6–121**, 6–153, F–74
  - Definition, F–58
  - Description, 6–136
- CNT<sub>AID</sub>, 8–11
- CNT<sub>MSC</sub>, 8–13
- Coding Conventions, F–63
- Coding of Service Packs Supported, **9–18**
- Coding of the Length Field, Description, F–6
- Coding of the Value Field, Description, F–6
- Combined Dynamic Data Authentication, ICS, R–4
- Combined Reader, 5–35, **5–39**, **5–40**, **5–41**, 10–6
- Command – Handler Overview, 8–5
- Command Key layout, **10–12**
- Command Keys, 4–16, 10–15
  - Description, 10–11
  - ICS, R–5
- Command keys, 10–11
  - Definition, **5–14**
- command keys, Vertically arranged, 10–15
- Command Overview, **8–2**
- Commands and Responses, Description, 8–1
- Comments and Explanations, ICS, R–10
- Communication errors, F–82
  - CAD and the Merchant Application, F–12
  - Public network, F–12
- Communication Handler, Description, 5–22
- Communication Protocols, Description, F–1
- Communication Session
  - Description, 6–140
  - Terms, 3–3
- Communication Statistics, Description, F–11
- Communication Statistics and Error Counters, 6–152
- Complete EMV Payment, 6–49
- Complete Key Entered Payment, 6–94
- Complete Payment, 6–74
  - Description, 8–48, 8–56, 8–62, 8–70
- Complete Payment command, 6–143
- Complete Token Based Payment, 6–107
- Completion Processing, ICS, R–9
- Configurable Kernel, ICS, R–1
- Configuration, 6–11
- Configuration and installation, 6–1
  - Configuration required, 6–6
  - Configure PSAM Application, Description, 8–16
  - Confirm Amount command, 6–152, 6–155
  - Connection Error Counter, F–17
  - Connection Errors, F–9
  - Connection Request, F–9
  - Connection Request counter, F–16
  - Connection Time counter, F–17
  - Contact force, 10–7, 10–8
  - Contacting elements, 10–7
  - Contacts, 10–7
  - Continuation Indicator, 6–11, 8–13
  - Continue using magstripe?, Merchant Display, 5–35
  - Counters, Example, **6–137**
  - Counters and Batch Numbers, Description, 6–129, 6–137
  - CRC, Abbreviations, 3–2
  - Create Service Record, Description, 8–26
  - Cryptogram Information Data, F–84
  - Cryptography, Introduction, 4–5
  - CTRL pin, 10–19
  - CURR
    - Get Amount, 8–80
    - Get Amount 2, 8–82, 8–83
    - Get Amount 3, 8–84, 8–85
  - CURR<sub>C</sub>, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66, G–5, G–6
    - Definition, 9–6
    - Get Debit/Credit Properties, 8–30
    - Local PIN, 8–88, 8–90
  - CURR<sub>E</sub>, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66
    - Definition, 9–6
    - Get Debit/Credit Properties, 8–30
    - Local PIN, 8–88, 8–90
  - Currency, 6–43
  - Currency Code, 5–15, 9–6, 9–21, G–5, G–6
    - Cashback, 7–16
  - Currency Exponent, Definition, 9–6
  - CV–2, 6–88, 8–75, 9–5, 9–7
    - Definition, 9–6
    - Field 47, F–83
  - CVC–2, 9–6
  - CVM, 2–1, 6–41, 6–50, 6–68, 6–88, G–24
    - Abbreviations, 3–2
  - CVM Capability, ICS, R–4
  - CVM Results, 6–53, F–84

CVM Status, 6–46, 6–92, 6–106, 8–41, 8–55,  
8–61, 8–69, G–25  
Coding, **9–7**  
Definition, 9–7  
Service Packs, 11–4  
Validate Data, 8–47

CVM Vs. Terminal Type, Best Practice, **7–22**

CVR, Abbreviations, 3–2

CVV–2, 9–6

CWI, **5–19**

## D

Danish Centre for Accessibility, Design requirements, 10–1

Danish Commerce & Services, Design requirements, 10–1

Danish letters, Display, 10–9

Danish Regulations, 4–5

Danish Text Translated into English (18 Characters per Line), **G–53**

Danish Text Translated into English (24 Characters per Line), **G–52**

Dankort, A–2, F–81, N–3

AID, 9–3

Terms, 3–3

Website, 3–11

Dankort Accelerated PIN Entry, Gavekort, I–2

Dankort Handbook, Introduction, 4–5

Dansk Center for Tilgængelighed, Design requirements, 10–1

Dansk Handel & Service, Design requirements, 10–1

DAPE

Abbreviations, 3–2

Dankort Accelerated PIN Entry, 6–54

Data Authentication, ICS, R–7

Data Link Layer, F–3

Data link layer, **F–2**

Data Management, Description, 10–24

Data Requested, 8–74

Coding, **9–7**

Definition, 9–7

Data Store, 4–16, 6–126, 6–131, 6–146,  
6–150, 10–20, 10–24

Defective, 7–15

Data Store Handler, Description, 5–21

Data Transmission, Best Practice, 7–9

Date, 8–24

Date Reconciliation, N–2

Date, local transaction, 6–119, F–85, N–2

DATE<sub>EFFECTIVE</sub>, 6–51, 8–37, 8–39, 8–65,  
8–67

DDA, 4–17, 4–25

Abbreviations, 3–2

DDOL, ICS, R–7

Deactivate PSAM, Description, 8–25

Declined, G–10

Declined Transaction, Receipt, G–12

Defective Advices, Description, L–1

Deleting records from File–5, L–3

Delta Electronics Testing, 4–26

DES, 4–5, 9–11, 9–25

DES and Triple DES, Notation, 3–5

Development Phases, Introduction, 4–26

DI, 5–19

Dialogue – Merchant and Cardholder, Gift Voucher, I–6

Differential Power Analysis, 5–12

Differential Power Analysis Attack, 10–14

Diners, N–3

Discretionary Data, **5–24**, 5–26, **A–1**

Get Debit/Credit Properties, 8–30

Display flow, M–6

Display Line for Host Message, Coding, F–15

Display Message Code, Get Amount 3, 8–84

Display Rules, 5–30

Display Texts, 5–15

Displays, 4–16

Document Overview, **4–4**

Documentation, 10–2

Download Control

Field 27, F–76

Position 1, **F–76**

Download Requirements, 10–25

DPA, 5–12

DTHR, 6–68, 6–88, 6–103

Dual Communication Platforms and Dual IP–Addresses, Best Practice, 7–17

Duplicate Transaction Check (PSAM), Best Practice, 7–13

Duplicate Transaction Time–out, Set D/C Properties, 8–33

Dynamic Data Authentication, 4–17, 4–25  
ICS, R–4

## E

ECBS, Abbreviations, 3–2

- ECR, Abbreviations, 3–2
  - EEPROM, 10–25
  - Eject Button, 10–16
  - EKSTRA, Receipt text, G–6
  - Electrical Design, Description, 10–16
  - Electrical environments, 10–1
  - Electrical Interfaces, Description
    - Cards, 10–19
    - PSAM, 10–18
  - Electrical Safety, Description, 10–17
  - Electromagnetic Compatibility, Description, 10–17
  - Electronically stored journals, 5–6
  - Embossing, 10–7
  - EMV, Abbreviations, 3–2
  - EMV Card Transactions, Description, 6–40
  - EMV Checksum, 6–2
    - Definition, 9–8
    - Get Debit/Credit Properties, 8–31
  - EMV level 1 test, 4–26
  - EMV level 2 test, 4–26
  - EMV Payment, Description, 8–40
  - EMVCo, 4–26, 5–2
  - Enciphered PIN Data
    - Local PIN, 8–91
    - Local PIN Validation, P–4
  - Enciphered PIN for offline Verification, ICS, R–4
  - Enciphered PIN for online Verification, ICS, R–4
  - End Sentinel, 9–11, 9–21, **A–1, A–2, A–3**
  - English texts, 5–15
  - Enter/Accept, 10–15
  - Envelope buffer size, Get Debit/Credit Properties, 8–31
  - Envelope Data
    - Maximum Length (EMV), Get Debit/Credit Properties, 8–31
    - Maximum length (MSC), Get Debit/Credit Properties, 8–31
  - Environmental conditions, 10–7
  - EPROM, 10–25
  - Error Counters, F–12
    - Description, F–11
  - Error Responses, 8–8
  - Error situations, Gavekort, I–7
  - Estimated Amount, 9–4
    - Get Amount 3, 8–85
  - Euro, Receipt, G–19
  - Europay, AID, 9–3
  - Event Handler, 6–2, 6–151
    - Description, 5–22
  - Example of Message Flow, Local PIN Validation, P–12
  - Exception File, ICS, R–8
  - Exception Handling
    - ICS, R–9
    - MAD–Handler, 5–6
    - Router, 5–4
  - Exception handling, 6–129, 6–146, 6–151
  - Exchange Debit/Credit Static Information, 6–8
    - Description, 8–19
  - Expiry Date, 6–88, 8–75, 9–5, 9–7, **A–1, A–2, A–3**
    - Definition, 9–8
  - Extra, K–1
  - Extra guardtime, **5–19**
- ## F
- Failed Transaction, Receipt, G–12
  - Fallback, 4–23, 5–31, 8–100, **F–68**, F–69
    - Best Practice, 7–3
    - Description, 5–33
    - Non–Debit/Credit, 5–34
    - Service Code, 5–34
    - Single Unit Terminal, S–6, S–7 to Key Entered, 4–23
    - to offline, 4–23
  - Fallback, Transaction Condition Code, G–24
  - Fallback Handling
    - Combined Readers, **5–39, 5–41**
    - Separate Readers, **5–37**
  - FCI, 6–42, 8–36, 8–38, 9–10
    - template, 6–42
  - FI, 5–19
  - Field 25, F–75
  - Field 39, 6–153
  - Field 46, 6–145, F–97
  - Field 55, F–84
  - Field 72, F–89
  - File Action Instruction, Definition, F–46
  - File Action Instruction Acknowledgement, Definition, **F–46**
  - FILEID<sub>ADMIN</sub>, Definition, 9–8
  - FILEID<sub>PRIORITY,n</sub>, Definition, 9–8
  - Final Amount Request, 9–3
    - Get Amount 3, 8–84

- Financial Advice, 6–124
    - Definition, **F–38**
  - Financial Request, Definition, **F–32**
  - Flash–PROM, 10–25
  - Floor limit, 4–8, E–2, F–75
    - CAT, E–2
  - Floor limit checking, ICS, R–8
  - Forced Acceptance, ICS, R–9
  - Forced CVM, 9–14
    - Best Practice, 7–5
  - Forced Offline
    - Best Practice, 7–6
    - Single Unit Terminal, S–8
  - Forced offline, 6–45, 6–71, 6–91, 9–14
  - Forced Online, 9–14
    - ICS, R–9
  - Fuel Dispensers, Introduction, 4–8
  - Full reversal, F–74
  - Function Code, **F–74**
    - APACS Header, F–6
    - Coding, F–14
    - Field 24, F–74
  - Function Keys, ICS, R–5
- G**
- Gavekort, Attachment I, I–1
  - Generation of a new Host Request, 6–147
  - Get Amount
    - Description, 8–80
    - Subsequent, 6–152
  - Get Amount 2
    - Best Practice, 7–12
    - Description, 8–82
    - Service Packs, 11–3
  - Get Amount 3
    - Best Practice, 7–12
    - Description, 8–84
    - Service Pack No. 2, 11–5
  - Get Amount command, 6–151, 6–155
  - DTHR, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66
    - Get Debit/Credit Properties, 8–30
  - Get Data, ICS, R–7
  - Get Debit/Credit File Characteristics, Description, 8–14
  - Get Debit/Credit Properties, Description, 8–28
  - Get Debit/Credit Properties Command
    - Local PIN Validation, P–10
    - Previous Transaction Status, Q–2
  - Get Event command, 6–67
  - Get Merchant Data, Description, 8–74
  - Get MSC Table, Description, 8–12
  - Get Next, Description, 8–18
  - Get PIN command, 6–152, 6–155
  - Get Supported AIDs, Description, 8–10
  - Gift Voucher, Attachment I, I–1
  - GMT, 6–136
  - GMT Offset
    - Field 15, F–64
    - Position 1, **F–64**
  - GODKEND, 10–15
  - Goods, ICS, R–5
  - Goods and Services, **7–24**, 9–23, F–64
    - Cash disbursement, **7–24**, 9–23, F–64
  - Grand Total, N–5
    - Field 46, F–82
  - Gratuity, 4–8, 6–17, 9–23, **G–4**, K–1
    - Best Practice, 7–16
  - Gratuity and other surcharges, 6–20
  - Guard Time, Complete Payment command, 5–4
  - Guidelines for evaluating the transaction result, **G–10**
- H**
- Hardware Requirements, Description, 10–13
  - Hardware Version Number, 6–123, 8–19, 8–21
    - Definition, 9–9
    - Field 46, F–82
  - HDLC, F–2
  - Hexadecimal, Notations, 3–4
  - Historical Characters, **5–19**, 9–17
  - Host Communication, F–1
  - Host Declined Transactions (Advices), 6–150
  - Host Declined Transactions (Requests), 6–147
  - Host Interface info, 6–2
  - Host Request, 8–22, 8–26, 8–41, 8–43, 8–47, 8–55, 8–61, 8–69
    - Definition, 9–9
  - Host Response, 8–22, 8–42, 8–44
    - Definition, 9–9
  - Hotel, 4–8, F–75, F–87



# I

- I-blocks, 5–19
- ICC Application Selection, Description, 5–28
- ICC Power–Off command, 6–49
- ICC Power–On command, 6–2
- ICC System Related Data, Field 55, F–84
- ICC technology and FallBack to Magnetic Stripe, Best Practice, 7–3
- ICCR, 10–5, 10–7
  - Abbreviations, 3–2
  - Description, 5–10
- ICS, R–1
  - Abbreviations, 3–2
- ID–000 format, 10–8
- ID–1 format, 10–8
- Identifier, 8–28, 8–32
  - Get Debit/Credit Properties, 8–30
  - Set Debit/Credit Properties, 8–33
- IDPP, 8–17
- IDPPCREATOR, 8–17
- IDPSAM, 8–10, F–85, G–8
  - Definition, 9–9
- IDPSAMAPP, 5–24, 5–37, 5–41, 6–2, 9–23
  - Definition, 9–9
- IDPSAMCREATOR, 8–10, F–85, G–8
  - Definition, 9–9
- IDScheme, 8–11
- IDSN, 6–123
- IDTHREAD, 6–143
- IFD, Abbreviations, 3–2
- IFSC, 5–18, 5–19
- IFSD, PSAM, 5–18
  - Value, 5–18
- Implementation Conformance Statement, Attachment R, R–1
- In–Flight Terminals, E–1, E–2
- INFO, 10–16
- Info, 6–28
- Info Level, 6–40, 6–87, 6–102, 6–119, 6–123, 8–19, 8–21
  - Coding, **9–10**
  - Definition, 9–10
  - Field 46, F–82
- Initial Amount Request, 9–3
  - Get Amount 3, 8–84
- Initialization Sequence, Normal flow, **6–4**
- Initiate EMV Payment, 6–41
  - Description, 8–35
- Initiate EMV Payment 2, Description, 8–37
- Initiate EMV Payment command, 6–43
- Initiate Key Entered Payment, Description, 8–57
- Initiate MSC Payment, Description, 8–49
- Initiate MSC Payment 2, Description, 8–51
- Initiate MSC Payment command, 6–69
- Initiate Payment 2 / Account Type, Service Packs, 11–8
- Initiate Token Based Payment, Description, 8–64
- Initiate Token Based Payment 2, Description, 8–65
- INS, Abbreviations, 3–2
- Install, Description, 8–21
- Install transaction required, 6–6
- Installation, 4–21, 6–1, 6–10, **6–121**, 6–145, 6–147, F–59, F–74
- Installation guide, 10–2
- Installation sequence, **6–4**
- Installation Transaction, **6–122**
  - Description, 6–121
- Integrated Circuit Card Reader, 4–15
  - Description, 10–6
- Integrated Circuit Cards, 5–23
- Interface Device Serial Number, **6–53**
- International Standards, Introduction, 4–2
- Internet Protocol, F–3
- IP, F–3, F–9
- IP–adress, 6–2
- ISDN, 7–17
- ISO/IEC, Abbreviations, 3–2
- Issuer Application Data, F–84
- Issuer Authentication, 6–47
- Issuer Authentication Data, F–85
- Issuer DD, Definition, 9–10
- Issuer Envelope, Set Debit/Credit Properties, 8–33
- Issuer Envelope Data
  - Definition, 9–10
  - Field 47, F–83
  - Set Debit/Credit Properties, 8–33
- Issuer Envelope Functionality, Service Pack No. 2, 11–7
- Issuer Envelope Response Data, Field 44, F–80

Issuer Script, 6–49  
 Issuer Script 1, F–85  
 Issuer Script 2, F–85  
 Issuer Script Results, F–84  
 Issuer-to-Card Script Processing, 6–47  
 Issuing the Get Amount 2 Command Twice,  
 Service Packs, 11–3  
 Issuing the Get Amount 3 Command Twice,  
 Service Packs, 11–5  
 ITA, 5–1

## J

JCB, 4–26, 4–27, 6–137, F–81

## K

KCV, 9–10  
 Abbreviations, 3–2  
 Local PIN, 9–25  
 KEK, Abbreviation, 3–2  
 KEK<sub>DATA</sub>, Coding, F–14  
 KEK<sub>PIN</sub> Version, Field 47, F–83  
 Key Check Value  
 Definition, 9–10  
 Local PIN, 9–25  
 Local PIN, 8–86  
 Key Entered Card Transactions, Description,  
 6–87  
 Key Entered Payment, 6–90  
 Description, 8–60  
 Key movement, 10–13  
 Keyboard Layout, 10–11  
 KØB, Receipt text, G–5  
 KSES<sub>DATA</sub>, Coding, F–14  
 KSES<sub>PIN</sub>, Field 47, F–83

## L

LAN, F–2  
 Landing contacts, 10–6, 10–8  
 Language Preference, 5–42  
 Language Selection  
 Description, 5–42  
 ICC, 5–42  
 Languages, 5–15

Last PIN incorrect  
 Definition, 9–25  
 Local PIN, 8–88, 8–90  
 Leap years, 10–5  
 LEN<sub>FCI</sub>, 6–42  
 Length of APACS 60 Message, Coding, F–14  
 LEN<sub>MSCD</sub>, Local PIN, 8–86, 8–88  
 Limitations, Previous Transaction Status, Q–5  
 Limited Amount Terminals, E–1  
 Limited-Amount Terminals, E–2  
 Load LP Keys Command, 8–86  
 Local PIN Validation, P–6  
 Load LP Keys Message Flow, Local PIN, **P–5**  
 Loading a Gavekort, Gavekort, I–5  
 Local PIN, P–1  
 ASW1–ASW2, 8–93  
 Best practice, 7–19  
 Local PIN Commands, 8–86  
 Local PIN Validation  
 Description, P–1  
 Message flow, P–2  
 Local PIN Validation Message Flow, **P–3**  
 Local PIN Verification, Description, 5–14  
 Local PIN Verification Status, Definition, 9–11  
 Lock, 10–7, H–9  
 Physical, 5–3  
 Technician, 5–3  
 Unattended terminal, H–7  
 Lodging, F–87  
 Log  
 Addendum record, 6–119  
 Additional Receipts for logging Purposes,  
 G–25  
 Description, 5–5  
 Log and Totals, Best Practice, 7–14  
 Log-information, File–5, L–3  
 Logging Devices, 4–17  
 Longitudinal Redundancy Check, **A–1, A–2,**  
**A–3**  
 LP-KEK  
 Definition, 9–25  
 Local PIN, 8–86  
 LP-KEK-Data, Local PIN, 8–86  
 LP-KEK-Version  
 Definition, 9–25  
 Get Debit/Credit Properties, 8–31  
 Local PIN, 8–86, 8–87  
 LP-Key, Definition, 9–25  
 LP-Key-Chain  
 Definition, 9–26

Local PIN, 8–87, 8–90  
 Local PIN Validation, **P–5**  
 LP–Key–Chain Structure, Local PIN, **P–6**  
 LP–Key–Version, Definition, 9–26  
 LP–PPK, Local PIN, 8–86  
 LP–PPK–Data, Local PIN, 8–86  
 LP–PPK–Version  
   Get Debit/Credit Properties, 8–31  
   Local PIN, 8–86, 8–87, 8–90  
 LRC, 5–9, 6–33, 9–11, 9–21  
   Abbreviations, 3–2  
 Luhn, 5–9  
 Luhn formula, B–1, I–15  
   Example, B–2

## M

MAC, **6–121**, 6–153, F–78, F–79  
   Abbreviations, 3–2  
 MAD, Abbreviations, 3–2  
 MAD–Handler, 4–15, 10–26  
   Description, 5–4  
   TAPA, 4–12  
 MAD–Handler ID, 6–119, 8–19, 8–21, 8–25,  
   F–83  
   APACS Header, F–6  
   Coding, F–16  
   Definition, 9–11  
   Field 46, F–82  
 Maestro, F–81  
 Magnetic Stripe, 5–33, F–68  
   Dankort, **A–2**  
   ICS, R–4  
 Magnetic Stripe Card Reader, 4–15  
   Description, 10–7  
 Magnetic Stripe Card Transactions, Description,  
   6–67  
 Magnetic Stripe Cards, 5–23  
 Magnetic Stripe Contents, Definition, 9–11  
 Mail order, F–69, G–24  
 Mail Order and Phone Order Environment,  
   Introduction, 4–8  
 Manual Cash Disbursement, Receipt, G–21  
 Marking, Description, 10–3  
 MasterCard, 4–26, 6–137, 9–6, 9–21, N–3  
   AID, 9–3  
 Max. PIN digits, Local PIN, 8–88, 8–90  
 Maximum PIN digits, Definition, 9–26  
 MCC, Abbreviations, 3–2  
 MDOL, Definition, 9–11  
 MDOL Data, Definition, 9–12  
 MDOL1, 6–44, 6–45, 6–70, 6–90, 6–92,  
   6–105, 8–37, 8–39, 8–40, 8–51, 8–53,  
   8–54, 8–59, 8–60, 8–65, 8–67, 8–68  
 MDOL2, 6–46, 6–72, 6–92, 6–93, 6–106,  
   6–107, 8–41, 8–42, 8–44, 8–55, 8–61,  
   8–69  
 ME No., **6–9**  
 ME<sub>ADDRESS</sub>, **6–9**, 8–20, G–5  
   Definition, 9–12  
 Mean Time Between Failures, 10–6  
 ME<sub>BRN</sub>, **6–9**, 8–20, G–5  
   Definition, 9–12  
 Mechanical Design, Description, 10–4  
 Mechanical environments, 10–1  
 ME<sub>CITY</sub>, **6–9**, 8–20, G–5  
   Definition, 9–12  
 ME<sub>NAME</sub>, **6–9**, 8–20, G–5  
   Definition, 9–12  
 ME<sub>NUMBER</sub>, 6–55, 6–105, 8–20, 8–65, 8–67  
   Definition, 9–12  
 ME<sub>PHONE</sub>, **6–9**, 8–20, G–5  
   Definition, 9–13  
 Merchant, 4–9  
 Merchant Address, Definition, 9–12  
 Merchant Application, 4–14, 6–143, 6–146  
   Description, 10–19  
 Merchant Application Handler, Description,  
   5–17, 6–37  
 Merchant Application Interface, Description,  
   10–8  
 Merchant Application Log, 6–9  
   Best Practice, 7–15  
   Exchange Debit/Credit Static Information,  
     8–19  
   Info Level, 9–10  
   Install, 8–21  
 Merchant Cancel Button, 6–154  
 Merchant categories, Addendum record,  
   6–118  
 Merchant Category Code, 3–2, **6–53**, 9–21  
 Merchant City Name, Definition, 9–12  
 Merchant Display, 5–35, 8–94, 9–23  
   Action Codes, **6–153**  
   Description, 6–37  
 Merchant Identifier, **6–53**  
 Merchant Initiated Actions, Description, 6–154

- Merchant Initiative, 6–118, 7–6, **9–14**, G–25
    - Best Practice, 7–5
    - Field 62, F–86
  - Merchant Initiative Bypass, O–1
  - Merchant Name, Definition, 9–12
  - Merchant Number, Definition, 9–12
  - Merchant Phone No., Definition, 9–13
  - Message Code, 6–146, 6–150, 6–152, **6–153**, 8–94
    - Assignments, 5–16
  - Message Number, Field 71, F–86
  - Message Reason Code, 6–9, **F–75**
  - Message Type, **F–4**
  - Message Type Identifier
    - APACS Header, F–6
    - Coding, F–14
    - Definition, 9–14
  - Messages for Display and Printing, **M–2**
  - Method Number
    - Definition, 9–26
    - Local PIN, 8–86, 8–88, 8–89, 8–90, 8–91
  - Method Specific Command Data, Local PIN, 8–86, 8–88
  - Method Specific Command Data , Local PIN, 8–90
  - Method Specific Response Data, Local PIN, 8–87, 8–89, 8–91
  - ME<sub>ZIP</sub>, **6–9**, 8–20, G–5
    - Definition, 9–13
  - MI, 6–45, 6–71, 6–91, 6–104, 6–118, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66
    - Definition, 9–13
    - Token, 6–28
  - Min. PIN digits, Local PIN, 8–88, 8–90
  - Minimum PIN digits, Definition, 9–26
  - Modulo 10, **A–2**, **A–3**, B–1
  - Modulo 11, **A–2**, **A–3**
  - Mounting of the PIN Entry Device, H–4
  - MRC, 6–119, 8–24
  - MSC, Abbreviations, 3–2
  - MSC Application Selection, Description, 5–27
  - MSC Payment, Description, 6–70, 8–54
  - MSC PIN Retry, Service Pack No. 1, 11–3
  - MSC Selection Record, Description, **5–24**
  - MSC Selection Table, 5–23
  - MSC Table, 6–11
  - MSCR, 5–9, 10–3, 10–7
    - Abbreviations, 3–2
    - Description, 5–8
  - MTBF, 10–6
  - MTI, **F–4**, F–85
    - Definition, 9–14
    - ISO notation, F–4
  - MTI of the Original Message, F–17
    - Definition, 9–15
  - MTI of the original message, APACS Header, F–6
  - multi language support, ICS, R–6
  - Multi–Application Driver Handler (MAD–Handler), 6–30
  - Multi–entry
    - Terminal Settings, 9–21
    - Terms, 3–3
- ## N
- Network Connection, **10–28**
    - Description, 10–27
  - Network Connection Type, F–9
    - APACS Header, F–6
    - Coding, F–15
  - Network Design, Description, 10–27
  - Network Layer, F–3
  - Network layer, **F–2**
  - Network Management Request, Definition, **F–59**
  - Network Model, Debit/Credit, **4–11**
  - New Application Data, 6–10
  - New application data, 6–1
  - New data available, 6–7
  - No CVM, 6–27
  - No CVM Required, ICS, R–4
  - No response from PBS, F–12
  - No–CVM, Additional logging, G–26
  - Noise, 10–5
  - Noise limits, **10–5**
  - Non–volatile, 10–24
  - Notation, 3–4
  - Number of card reader errors, Field 46, F–82
  - Number of Entries, Previous Transaction Status, Q–6
  - Number of Fatal Errors, Field 46, F–82
  - Number of PIN tries left
    - Definition, 9–26
    - Local PIN, 8–88, 8–90
  - Number of System Faults, Field 46, F–82

Number of time-outs, Field 46, F-82  
 Number of unsupported cards, Field 46, F-82  
 Numeric Keys, ICS, R-5  
 Numeric layout, Keyboard, 10-11

## O

Odd parity, 5-8  
 Offline, 4-22  
 Offline Data Authentication, 6-41  
 Online, 4-22  
 Online Transactions, Description, 6-139  
 Online/Offline Transactions Vs. Terminal Type, Best Practice, 7-21  
 Operational Regulations, 4-6  
 Operators, Notation, 3-5  
 OPT, 5-1  
 Optimizing the Transaction Time, 6-54  
   Best Practice, 7-8  
 Original Authorization, 6-15, G-5, K-1  
   Info Level, 9-10  
   Receipt, G-13  
 Original Authorization with PIN or Combined CVM, Receipt, G-39  
 Original Data Elements, Field 56, F-85  
 OTA, 5-1  
 Out of Paper, 5-7

## P

Pad Synchronization Sequence, 6-13  
 Padding, Local PIN, 8-91  
 PAN, 5-23, 6-44, 6-70, 6-75, 6-88, 6-90, 6-105, 6-119, 8-24, 8-37, 8-39, 8-51, 8-53, 8-59, 8-65, 8-67, 8-71, 8-75, 9-5, 9-7, **A-1**, **A-2**, A-3, B-1, G-25, Q-1  
   Abbreviations, 3-2  
   Definition, 9-15  
   Get Amount 2, 11-3  
   Get Amount 3, 8-84  
   Get Debit/Credit Properties, 8-30  
   Previous Transaction Status, Q-5, Q-6  
   Printing, G-23  
   Ranges, 5-27, 6-1  
   Receipt, 6-50  
   Receipt text, G-6  
   Truncation, G-23  
 PAN Seq. No., Get Amount 3, 8-84  
 PAN Sequence Number, Definition, 9-15

PAN-prefix, 4-18  
   Best Practice, 7-12  
   Get Amount 2, 8-82, 11-3  
   Service Packs, 11-3  
 PAN<sub>FROM</sub>, 8-13  
   Definition, 9-15  
 PAN<sub>SEQUENCE</sub>, 8-37, 8-39, 8-65, 8-67, G-6  
 PAN<sub>TO</sub>, 8-13  
   Definition, 9-15  
 PAP, F-3  
 Paper Low, 5-7  
 Parallel Processing, Best Practice, 7-8  
 Parity, 6-33  
 Partial AID, ICS, R-6  
 Partial reversal, F-74  
 Passenger Transport, F-87  
 Password, 5-3, 5-21, H-8, L-3  
 Patent Issues, 5-2  
 PBS, 4-26, 5-25, 9-12  
 PBS A/S, Address, Z-1  
 PBS Debet/Kredit, 9-23  
 PBS NR, Receipt text, G-7  
 PBS PSAM, Terms, 3-3  
 PDOL, 6-52, 11-3  
 PED, 4-13, 4-17, 4-26, 10-13  
   Abbreviations, 3-2  
 PED info, 6-2  
 PED Software, 10-15, 10-21  
   Audit, 10-23  
   Handling of Alarms, 10-23  
   Implementation and Maintenance, 10-22  
   Installation, 10-22  
 Phasing out old Terminals, 4-26  
 Phone order, G-24  
 Physical Layer, F-2  
 Physical layer, **F-2**  
 Physically Secure Device, Definition, 5-11  
 PI Card Type, **A-2**, **A-3**  
 Pick up, 8-107  
 Pick-up, 8-72, 9-19  
 Pictograms, 10-3  
   Examples, 10-4  
 PIN, 5-3, 6-151, E-2  
   Abbreviations, 3-2  
   Capture, F-67  
   Capture capability, **F-66**  
   Data, Definition, 9-15  
   Digit, Representation, **5-13**

- Management, 5–12
- Privacy, 10–12
- Retry, 6–147, 11–3
- Retry Flow, 6–149
- Tries, Local PIN, P–10
- PIN Block Format, Field 47, F–83
- Pin connector, 10–8
- PIN Entry, 6–25, 6–43, 6–70, M–7
  - Device, 4–16, 10–13, H–1
  - Numeric Keys, H–2
- PIN or No CVM, Receipt, G–30
- PIN Pad, 10–2, F–69
  - Keyboard, 5–12
  - Software, 10–25
  - Description, 10–11
  - Field 46, F–82
  - ID, 5–12
  - Introduction, 5–11
- PIN Pad Data, Storage, 10–24
- PIN Pad layout, 10–12
- PIN Pad Software, 10–26
- Exception Handling, 6–143, 6–145, 6–147
  - Description, 6–143
- PIN– and No–CVM based Transactions, Additional logging, G–26
- PIN–based Terminals, Introduction, 4–2
- PIX, 9–3
- PK, Abbreviations, 3–2
- Placement and Installation of the terminal, H–4
- Placement of the terminal, H–5
- Plaintext PIN Block, **P–4**
  - Local PIN, 8–91
- Plaintext PIN Data, Local PIN Validation, P–4
- Plaintext PIN for ICC Verification, ICS, R–4
- Point of Service, Terms, 3–3
- POS, Abbreviations, 3–2
- POS Capability, **F–70**
- POS Capability Code, 6–123, 8–19, 8–21
  - Definition, 9–16
  - Field 21, F–64
  - Position 1, **F–65**
  - Position 2, **F–65**
  - Position 3, **F–65**
  - Position 4, **F–65**
  - Position 5, **F–66**
  - Position 6, **F–66**
- POS Capability Codes, **F–72**
- POS Entry Mode, 5–35, 6–42, **6–53**, 6–68, 6–89, 8–36, 8–38, 8–47, 8–50, 8–52, 8–58, 8–64, 8–66, 9–21, **F–70**, **F–72**, G–25
  - Definition, 9–16
  - Field 22, F–67
  - Initiate Payment command, **F–69**
  - Position 1, **F–68**
  - Position 2, **F–68**
  - Position 3, **F–68**
  - Position 4, **F–68**
  - Position 5, **F–69**
  - Position 6, **F–69**
  - Service Packs, 11–4
  - Token, 6–28
- POS terminal, 10–6
- POS Terminal/CAT Levels vs. Terminal Type, Best Practice, 7–21
- Postal Code, 9–13
- Power failure, 10–7, 10–17
- Power On, Description, 6–2
- Power Supply, 10–19
  - PSAM, 5–19
- Power supply, 10–17, 10–18
- Power–on, Type of Application, 9–23
- PP, Abbreviations, 3–2
- PPK, Abbreviation, 3–2
- PPP, F–3
- PPS, 5–19, 10–18, 10–19
  - Abbreviations, 3–2
  - ICC, 5–10, 5–11
  - PSAM, 5–18
- Presentation layer, **F–2**
- Previous Transaction Status, Get Debit/Credit Properties, 8–30
- Primary Account Number, 5–23, 9–15, B–1
  - Gavekort, **I–15**
- Primary and Secondary Call Numbers, F–1
- Printer, 5–14, 6–37
- Printing, 5–5, 6–30
- Priority1 file, 6–124
- Priority2 file, 6–124
- Priority3 file, 6–124
- Priority4 file, 6–124
- Privacy Shield, H–1
  - Height and position of the PED, **H–14**
  - Height of the Shielding, **H–12**
  - Mounting of the PED, **H–13**
  - PIN Entry Device, **H–10**
  - Reference Directions, **H–11**
  - Size and Orientation, H–1
- Privacy shield, 10–11
- Problem Reporting, Description, Z–1

- Processing Code, Field 3, **F–63**
  - Processing Option Data Object List, **6–52**
  - Processing Restrictions, **6–41**
  - PROM, **10–25**
  - Properties / Data Elements to be Set, Set Debit/Credit Properties, **8–33**
  - Proprietary Application Identifier Extension, Definition, **9–3**
  - Proprietary Data
    - APACS Header, **F–6**
    - Coding, **F–16**
  - Protocol Layers, **F–2**
  - Protocols, Description, **F–1**
  - PSAM
    - Abbreviations, **3–2**
    - Receipt text, **G–8**
  - PSAM Behavior for Variants of different Get Amount Commands, **11–7**
  - PSAM busy, **6–147**
  - PSAM Card Reader(s), Description, **10–8**
  - PSAM clean-up, **6–143**
  - PSAM Code Checksum, **6–2**
    - Definition, **9–16**
  - PSAM Config Checksum, **6–2**
    - Definition, **9–16**
  - PSAM D/C Life Cycle State
    - Definition, **9–17**
    - Get Debit/Credit Properties, **8–30**
  - PSAM Date, Field 46, **F–82**
  - PSAM Deactivation, **4–21**, **6–121**, **6–136**
    - Definition, **F–62**
    - Description, **6–135**
  - PSAM deactivation, **F–74**
  - PSAM Declined Offline Transactions, Definition, **6–150**
  - PSAM Declined Online Transactions, Definition, **6–150**
  - PSAM Handler, Description, **5–17**
  - PSAM ID, **6–2**
    - APACS Header, **F–6**
    - Coding, **F–14**
    - Field 60, **F–85**
  - PSAM Identifier, Get Debit/Credit Properties, **8–30**
  - PSAM Life Cycle State, Field 46, **F–82**
  - PSAM Related Errors, Definition, **6–147**
  - PSAM Scripts, **6–139**
  - PSAM Shutdown
    - Command, **6–146**
    - Description, **6–14**
  - PSAM Software, **10–26**
  - PSAM State Information, **6–10**
    - Exchange Debit/Credit Static Information, **8–19**
    - Install, **8–21**
  - PSAM Subversion, **6–2**
    - Definition, **9–17**
    - Get Debit/Credit Properties, **8–30**
  - PSAM Update, **4–21**, **6–121**, **6–129**, **6–135**, **6–147**
    - Definition, **F–61**
    - Description, **6–133**, **8–34**
    - Field 63, **F–86**
    - Messages, **F–46**
  - PSAM update, **F–74**
  - PSAM Version
    - Definition, **9–17**
    - Field 46, **F–82**
    - Get Debit/Credit Properties, **8–30**
  - PSAM version no., **6–2**
  - PSAM/PIN Pad Synchronization, **6–12**
  - PSAM/PIN Pad synchronization, **6–1**
  - PSAMs, TAPA, **4–13**
  - PSE selection, ICS, **R–6**
  - PSN, Receipt text, **G–6**
  - PSTN, **7–17**
  - Pull-up resistor, **10–19**
  - Purchase, **4–19**, **6–14**, **G–5**, **K–1**
- ## Q
- Quality Handbook, **5–2**
  - Quasi-cash and scrip, **7–24**, **9–23**, **F–64**
- ## R
- Random Number, **6–126**, **6–150**
    - Field 61, **F–86**
  - Random Pad Pattern, Local PIN, **8–91**
  - Random Transaction Selection, ICS, **R–8**
  - Receipt, Presence of Data Elements, **G–11**
  - Receipt – Failed, **G–12**
  - Receipt – Reversal, **G–16**
  - Receipt – Transaction Stopped by Attendant, **G–16**
  - Receipt overview, **G–4**

- Receipt Printer, 4–16
    - Description, 10–16
  - Receipt Variants, Description, G–9
  - Receipts
    - 18 characters per line, G–44
    - Best Practice, 7–11
    - Description, G–1
    - Gavekort, I–8
  - Receipts in English, Receipts, G–52
  - Receipts to be printed Vs. Business Environment, **G–28**
  - Reconciliation counter id, **F–80**
    - Description, 6–137
  - Reconciliation counter name, F–80
    - Description, 6–137
  - Reconciliation date, Description, 6–137
  - Reconciliation id, **F–80**
  - Reconciliation Indicator, N–2, N–3
    - Description, 6–137
  - REF, Receipt text, G–9
  - Reference STAN, F–17, N–7, Q–1
    - APACS Header, F–6
    - Definition, 9–17
    - Get Debit/Credit Properties, 8–30
    - Previous Transaction Status, Q–3
  - References, 3–7
  - Referral, G–24
  - Refund, 4–20, 6–19, G–5, G–7, **G–24**, K–1
    - Application Selection, 7–4
  - Refund (Signature), Receipt, G–33
  - Refund Transactions, Additional logging, G–26
  - Registered Application Identifier, 9–3
  - Registration No., **A–2**, A–3
  - Rejected Signature, Receipt, G–13
  - Rejection tone, 10–10
  - Release of the ICC, 6–56
    - Best Practice, 7–9
  - Release of Token – Reversal (Authorization), Receipt, G–40
  - Reliability, 10–6
  - Repeat Last ICC Response
    - Description, 8–79
    - FCI, 6–42
  - Repeat Messages, 6–139
  - PIN, 6–35
    - Length, 6–25
    - Tries, 6–35
  - Requirements from Third Parties, 10–2
  - Reset , CAD, 5–22
  - Response Code, 5–10, 6–151, 6–155, 11–4
  - Response time for previous online transaction, Field 46, F–82
  - Restart, 6–1
    - Description, 6–6
  - Restart required, 6–7
  - Restaurants, 4–8
  - Retail Environment, Introduction, 4–7
  - Retrieval Reference Number, 6–137
  - Retrieve Local PIN Information, Get Debit/Credit Properties, 8–31
  - Returns/☒ **7–24**
  - Returns/Refunds, 9–23, F–64
  - Reversal, 6–145
    - Advice, 5–36, 6–150
    - Definition, **F–48**
    - Authorization, 4–20, 6–18, K–1
  - Reversal (Authorization), 6–28
    - Receipt, G–15
  - RFU, Abbreviations, 3–2
  - RID, 9–3
    - Abbreviations, 3–2
    - PSAM, 8–10, F–85
  - RID<sub>PSAM</sub>, Definition, 9–17
  - Router
    - Description, 5–4
    - TAPA, 4–12
  - RSA, 10–26
- ## S
- SAM, Abbreviations, 3–2
  - Scanned Bar Code Data, Gavekort, **I–15**
  - SDA, 4–17
    - Abbreviations, 3–2
  - SDL Notation, Description, C–1
  - Search Keys, Previous Transaction Status, Q–1
  - Secure Cryptographic Device, 5–12, 10–13
    - Definition, 5–11
  - Security, Introduction, 4–24
  - Security Capability, ICS, R–4
  - Security Handbook, 5–2
  - Security Mechanism, 6–126
  - Security Zones, 4–24, **4–25**
  - Segment Number, 8–42, 8–44, 9–24
  - Self–Service Terminals, E–1, E–2
  - Separate Reader, 5–37



- Separator, **A–1, A–2, A–3**
- Service Code, 5–32, 5–33, 5–36, **A–1, A–2, A–3**
  - Definition, 9–18
  - Get Debit/Credit Properties, 8–30, 8–31
- Service life, 10–7
- Service Pack Check, **6–8**
- Service Pack No. 1, 11–2
  - Best Practice, 7–12
- Service Pack No. 2, 11–5
  - Best Practice, 7–12
- Service Packs, 11–1
  - Best Practice, 7–4
  - Restart, 6–7
- Service Packs requested, 6–2
- Service Packs Supported, Definition, 9–18
- Service Packs supported, Get Debit/Credit Properties, 8–30
- Service Record, 6–134, F–57, F–74
- Services, ICS, R–5
- Session Layer, F–3
- Session layer, **F–2**
- Set Debit/Credit Properties
  - Description, 8–32
  - Service Pack No. 2, 11–7
- SHA–1, 6–126
- Shielding
  - Design Recommendations, H–3
  - Size and orientation, H–1
- Shoulder Surfing, H–1
- Shut–down, 6–146
- Shutter, 10–8
- Signature, 6–26
- Signature (paper), ICS, R–4
- Signature accepted, 6–49, 6–74
- Signature accepted?, Best Practice, 7–10
- Signature based Transactions, Additional logging, G–26
- Signature or Combined CVM
  - After adding Extra Amount, G–37, G–41
  - Possibility for adding Extra Amount, G–35, G–42
  - Receipt, G–31
- Signature Status, 8–73
- Signature Validation, Best Practice, 7–11
- Signature Verification
  - Coding, **9–18**
  - Definition, 9–18
- Signature Verification and Accept, 7–10
- Signature Verification Function, 6–26
- Signature–based Terminals, Introduction, 4–2
- Single Unit Terminal
  - Terms, 3–3
  - Transaction Flow, **S–3**
- Single–layer paper, G–17
- SLET, 10–15
- SLET ALT, 10–15
- Sliding contacts, 10–8
- Software Design, Description, 10–20
- Software download, 10–26
- Software Version Number, 6–123, 8–19, 8–21
  - Definition, 9–18
  - Field 46, F–82
- SPA, 5–12
- STAN, 6–51, 6–75, 6–105, 6–118, 6–147, 8–24, 8–37, 8–39, 8–43, 8–47, 8–51, 8–53, 8–59, 8–65, 8–67, F–82, G–9
  - Definition, 9–19
  - Receipt text, G–7
- Standard Layout, 18 characters per line, G–46
- Start Sentinel, 9–11, 9–21, **A–1, A–2, A–3**
- Start–up, 6–145, 6–147
- Start–up PSAM, 6–6
  - Description, 8–9
- State Information, 8–76, **9–10**
- Static Data Authentication, 4–17
  - ICS, R–4
- Static discharge, 10–18
- Statistic Vector, F–16, **F–18**
- Statistics, 6–68, 6–89, 6–104, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66, F–6, F–9
  - Candidates tags, F–82
  - Coding, F–16
  - Definition, 9–19
  - Description, F–11
  - Initiate EMV Payment, 6–42
- STATUS, Receipt text, G–8
- Status of Previous Transactions, Q–1
- Status of Previous Transactions (Terminal), Best Practice, 7–14
- STIP, 5–1
- Stop List, 6–45, 6–71, 6–91, 6–150
  - Best Practice, 7–8
  - Electronic data file, 6–44, 6–71, 6–90
  - Manual look up, 6–44, 6–71, 6–90
- Stop List check, 6–44
- Stop List Status, 6–44, 6–45, 6–71, 6–91, 8–72
  - Coding, **9–19**

- Definition, 9–19
  - Storage of Data, Description, 10–24
  - Storage of Data Elements, **6–53**
  - Storage of Software, 10–25
  - String, Notation, 3–4
  - Structure of the Tag Field, F–5
  - Supplementary Authorization, 6–16, 8–69, K–1
  - Support of Card Technologies, Best Practice, 7–3
  - Support of Cardholder Verification Methods, Best Practice, 7–5
  - Surcharges, Best Practice, 7–16
  - Synchronization, 6–12
  - Synchronize PSAM/PIN Pad, Description, 8–17
  - System Trace Audit Number, 9–19
  - Systems Trace Audit Number, 6–119, 6–147, F–14, F–85
    - APACS Header, F–6
- T**
- T=0 protocol, 5–11
  - T=1 protocol, 5–11, 5–17, 5–18
  - Tactile identifier, 10–13
  - Tag
    - 4F, 9–3
    - 50, 5–30, 6–51, 9–4
    - 57, F–20, F–32, F–38, F–40, F–48, F–50
    - 5F24, 9–8, F–20
    - 5F2A, F–84
    - 5F2D, 5–42
    - 6F, 6–42
    - 70, 8–102
    - 71, F–85
    - 72, F–85
    - 82, F–84
    - 84, 9–3
    - 8A, F–84
    - 91, F–85
    - 95, F–84
    - 9A, F–84
    - 9B, F–84
    - 9C, F–84
    - 9F02, F–84
    - 9F03, F–84
    - 9F10, F–84
    - 9F11, 5–30
    - 9F12, 5–30
    - 9F1A, F–84
    - 9F1C, 9–20
    - 9F26, F–84
    - 9F27, F–84
    - 9F33, F–84
    - 9F34, F–84
    - 9F36, F–84
    - 9F37, F–84
    - 9F4B, 8–98
    - 9F53, 9–21
    - A3, F–80
    - A4, F–80
    - A5, F–80
    - BF0C, 9–10
    - C0, 1–7, F–6, F–14
    - C1, F–6, F–14
    - C2, F–6, F–14
    - C3, F–6, F–14
    - C4, F–6, F–14, N–7
    - C5, F–6, F–14
    - C6, F–6, F–14
    - C7, F–6, F–14
    - C8, F–6, F–15
    - C9, 7–18, F–6, F–15
    - CA, 7–18, F–6, F–15
    - CB, F–6, F–8, F–9, F–15
    - CC, F–6, F–16
    - CD, F–6, F–16
    - CE, F–6, F–16
    - CF, 1–7, F–6, F–8, F–16, F–18
    - D0, F–84
    - D1, 9–17, F–6, F–17, N–7
    - D2, F–6, F–17, N–9
    - E0, F–5, F–6
    - E2, F–6
    - E6, I–3
    - I1, F–63
    - IM, F–63
    - M4, I–3
    - T1, F–80
    - T2, F–82
    - T3, F–82
    - T4, F–82
    - T5, F–82
    - T6, F–82
    - T7, F–82
    - T9, F–82
    - TA, F–82
    - TB, F–82
    - TC, F–82
    - TD, F–82
    - TE, F–13, F–82
    - TF, F–13, F–82
    - TG, F–82
    - TH, F–13, F–82
    - TI, F–82
    - TJ, F–82
    - TK, F–82
    - TL, F–83
    - TM, F–83
    - TN, F–83
    - TO, F–86
    - TP, F–82
    - TQ, F–82

- TR, F–82
- TS, F–82
- TX, 11–8, F–83
- TY, 11–8, F–80
- V5, F–83
- Tags, Messages and related Tags, **F–97**
- Tamper Evidence, 10–13
- Tamper Evident Device, 5–12
- Tamper Resistance, 10–14
- Tamper Response, 10–14
- TAPA, 4–3, 4–11, 5–1, 6–1, 6–14, 6–40, 8–8
- TAPA Architecture, Local PIN, **P–2**
- TAPA Model, 4–13
- TAPA PSAM Application Identifier, Definition, 9–9
- Tapping Device, H–1
  - Countermeasure, H–8
- TC, 5–36, 6–46, F–84
  - Abbreviations, 3–2
- TC1, 5–19
- TCK, **5–19**
- TCP, F–3, F–9
- TDOL, ICS, R–9
- TED, 6–35
- Telephone order, F–68, F–69
- Temporary Offline Procedure, Best Practice, 7–6
- Temporary use with records, File–5, L–4
- TERM, Receipt text, G–6
- Terminal, Physical Implementation, **4–14**
- Terminal Action Analysis, 6–44
  - ICS, R–8
- Terminal Approval No., 6–119, 6–123, 8–19, 8–21, 8–24, 8–25
  - Definition, 9–19
  - Field 46, F–82
  - Service Packs, 11–1
- Terminal Architecture for PSAM Applications (TAPA), **4–12**
- Terminal Capabilities, **6–53**, 6–123, 8–19, 8–21, F–84
  - Field 46, F–82
- Terminal capabilities, ICS, R–4
- Terminal Categories, Best Practice, 7–1
- Terminal Checksum
  - Definition, 9–20
  - Get Debit/Credit Properties, 8–31
- Terminal Country Code, F–84
  - ICS, R–3
- Terminal Currency Code, ICS, R–3
- Terminal Data, Storage, 10–24
- Terminal Data Input Capability, ICS, R–5
- Terminal Data Output Capability, ICS, R–6
- Terminal Floor Limit, 6–53
- Terminal Identification, 6–42, 6–53, 6–68, 6–88, 6–104, 6–119, 6–123, 8–24, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66, G–6
  - APACS Header, F–6
  - Coding, F–16
  - Definition, 9–20
- Terminal Manufacturer ID, 9–11, F–83
  - Definition, 9–20
- Terminal Merchant Table, **6–9**
- Terminal Model, 4–11
- Terminal Operator, 4–9, 10–25
  - Terms, 3–3
- Terminal Operator Communication Access Points, 6–142
- Terminal Related Errors, Definition, 6–145
- Terminal Risk Management, ICS, R–8
- Terminal Serial Number, 9–11, F–83
  - Definition, 9–20
- Terminal Settings, **9–21**
  - Definition, 9–20
  - Set Debit/Credit Properties, 8–33
- Terminal Software, 10–25
- Terminal Software Modules, 10–26
- Terminal Software version no., 6–2
- Terminal Supplier, 5–21, 10–25
  - Terms, 3–3
- Terminal Type, 4–7, 6–123, 8–19, 8–21
  - Field 46, F–82
  - ICS, R–3
- Terminal Types, Best Practice, **7–25**
- Terminal Verification Result (TVR), F–84
- Terminals with☐
  - Merchant Interface, Attachment S, S–1
- Terms, Translation, K–1
- Test House, Terms, 3–3
- Text Written in Grey, Notation, 3–5
- The fifth File (File–5), L–2
- Thermal
  - Design, 10–5
  - Requirements, **10–6**
- Time, 8–24
  - Definition, 9–27

- Time, local transaction, 6–119, F–85, N–2
- Time-out, 5–42, 6–151, 6–154, 11–4, F–75
- Ttime-out value, Duplicate Transaction Check, 7–14
- Timer Flag, Definition, 9–27
- Timing Attack, 10–14
- Timing attack, 5–12
- TIP, 4–26
- TLV, 6–42, 6–52, F–84
  - Coding, F–5
- Token, 6–27
  - Complete Payment, 8–49, 8–57, 8–63, 8–71
  - Definition, 9–21
  - Format of the Token, 6–28, **6–30**
  - Maximum length, 6–29
  - POS Entry Mode, **F–69**
  - Retrieval of the Token, 6–29
  - Terms, 3–3
- Token Based Payment, Description, 8–68
- Token based Transactions, 6–102
- TOTAL, Receipt text, G–6
- Total Reports
  - Description, F–17, N–1
  - Gavekort, I–16
- TR, 6–41, 6–68, 6–88, 6–104, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66, 9–22
- Track1, 5–8
- Track2, 5–8, 5–9, 6–68, 6–87, **A–1**
  - Data, 5–35, 8–50, 8–52, 9–11
  - Definition, 9–21
  - Get Debit/Credit Properties, 8–30
- Track3, 5–8
- Transaction, Terms, 3–4
- Transaction Category Code, Definition, 9–21
- Transaction Checks, Best Practice, 7–13
- Transaction Completed command, 6–75, 6–94
- Transaction Condition Codes, **G–24**
- Transaction Counter
  - Definition, 9–27
  - Get Debit/Credit Properties, 8–31
  - Local PIN, 8–91
- Transaction Counter Validation, Local PIN Validation, P–8
- Transaction Currency Code, F–84
- Transaction Date, F–84
- Transaction flow, 6–39
- Transaction Gratuity Amount, Definition, 9–21
- Transaction Log, ICS, R–8
- Transaction Request, F–17
  - Coding, **9–22**
  - Definition, 9–22
- Transaction Request Vs. Terminal Type, Best Practice, **7–23**
- Transaction Requests and Totals Affected, **N–6**
- Transaction Result, Best Practice, 7–13
- Transaction Sequence Number, 6–53
- Transaction State Information, 6–50, 6–70
  - Best Practice, 7–18, 7–19
  - Coding, **9–22**
  - Command, 6–40, 6–72, 6–87, 6–92, 6–106
  - Definition, 9–22
  - Description, 8–76
- Transaction Status, 6–27, 6–49, 6–74, 6–94, 6–119, 6–143, 8–48, 8–56, 8–62, 8–70
  - Coding, **9–23**
  - Definition, 9–23
- Transaction Status Information, F–84
- Transaction Stopped/Canceled, Receipt, G–16
- Transaction Time, 6–53
- Transaction Total Amount, Definition, 9–23
- Transaction Type, 4–19, 6–42, **6–53**, 6–104, F–84
  - Definition, 9–23
- Transaction Type Vs. Terminal Type, Best Practice, **7–24**
- Transaction Types, Previous Transaction Status, Q–5
- Transfer of records from File–5, L–2
- Transmission Factors F and D, Best Practice, 7–10
- Transmission Flows, F–3
- Transmission Formats, Description, F–4
- Transport Layer, F–3
- Transport layer, **F–2**
- Truncation of PAN digits, **G–24**
- TSI, **6–53**, F–84
- TT, 6–42, 6–68, 6–89, 6–104, 8–36, 8–38, 8–50, 8–52, 8–58, 8–64, 8–66, 9–23
- TVR, **6–53**, F–84
- Type A Transactions, CAT Levels, E–1
- Type B Transactions, CAT Levels, E–1
- Type C Transactions, CAT Levels, E–1
- Type of Application, Definition, 9–23
- Type of application, 6–2

## U

- Unattended Terminals, Receipts, G–14

Unique serial number, 10–3  
Unpredictable Number, 6–53, F–84  
Unsupported cards, F–12  
Update Data, 8–34  
    Definition, 9–24  
Update Number, 8–34  
    Definition, 9–24  
Update Results, Field 46, F–82  
User Guidance, 10–3  
User Interface, 6–155  
User Interface Display, Description, M–1  
User Interface Handler, Description, 5–11,  
    6–31

## V

V.110, F–2  
V.120, F–2  
Application Chaining, 8–46  
Validate Data, 6–47, 6–73, 6–93  
    Description, 8–41  
Validate Data 2, 8–44  
    Service Pack, 11–4  
Validate Install Data, Description, 8–22  
Validate Install Data command, 6–123  
Validation of the PAN, B–1  
Vehicle Rental, F–87  
Velocity Checking, ICS, R–8  
Verify Signature, Description, 8–72  
Verify Signature command, 6–51, 6–76, 6–95

Viewing angle, 10–10  
Visa, 4–26, 9–6  
    AID, 9–3  
Visa/Dankort, Terms, 3–4  
Visual Indicators, Description, 10–9  
Voice Authorization, 6–45, 6–71, 6–72, 6–91,  
    8–72, 9–19  
    Definition, 3–4  
Voice Authorization Call, Single Unit Terminal,  
    S–8  
Voice Authorization Calls, 7–7  
VPKI, Abbreviations, 3–2  
VPN, F–2

## W

Waiting Time Extension, 5–19  
Waivers  
    Procedure for obtaining, 4–27  
    Template, 4–27  
Websites, 3–11  
Write Handler String command, 6–50, 6–94  
WTX, PSAM, 5–19

## X

X.75, F–2  
XMODEM protocol, 10–20

## Z

ZIP code, 9–13

**This page is intentionally left blank**