AEIPS
Terminal Technical Manual
(AEIPS 4.3)

April 2015

American Express

Confidential and Trade Secret Materials

This document contains sensitive, confidential and trade secret information and may not be disclosed to third parties without the prior written consent of American Express Travel Related Services Company, Inc.

The policies, procedures, and rules in this manual are subject to change from time to time by American Express Global Network Services.

Table of Contents

1 SUMMARY OF CHANGES 10

2 INTRODUCTION 11

2.1 Scope 11

2.2 Audience 11

2.3 Reference Materials 11
2.3.1 ISO 11
2.3.2 EMV 12
2.3.3 American Express 12

2.4 Use of Terms 12
2.4.1 Optional, Mandatory or Conditional 12
2.4.2 Use of the Term “Chip Card” 12
2.4.3 Cardholder or Cardmember? 12

2.5 Document Structure 13

2.6 Notation 13

3 TRANSACTION OVERVIEW 14

3.1 Functional Overview 14

3.2 Dual Interface Support 15

3.3 Mandatory and Optional Functionality Summary 15
3.3.1 Functions 15
3.3.2 Commands 16
3.3.3 AEIPS Command Non-Specific Status Words 17

4 APPLICATION SELECTION 18

4.1 Overview 18

4.2 Commands 18

4.3 Processing Requirements 19
4.3.1 Chip Card Insertion and Power Up Sequence 19
4.3.2 Answer to Reset 19
4.3.3 Application Selection – Building the Candidate List 19
4.3.4 Application Selection – Choosing the Required Application 20

5 INITIATE APPLICATION PROCESSING 21

5.1 Overview 21

5.2 Commands 21

5.3 Processing Requirements 21

6 READ APPLICATION DATA 23

6.1 Overview 23

6.2 Commands 23

6.3 Processing Requirements 23

7 OFFLINE DATA AUTHENTICATION 25

7.1 Overview 25
7.1.1 Static Data Authentication (SDA) 26
7.1.2 Dynamic Data Authentication (DDA) 27
7.1.3 Combined DDA / Application Cryptogram Generation (CDA) 27

7.2 Commands 27

7.3 Processing Requirements 28
7.3.1 American Express Scheme CA Keys 28
7.3.2 Static Data Authentication (SDA) 28
7.3.3 Dynamic Data Authentication (DDA) 29
7.3.4 Combined DDA/AC Generation (CDA) 29

8 PROCESSING RESTRICTIONS 30

8.1 Overview 30

8.2 Processing Requirements 30

9 CARDHOLDER VERIFICATION 32

9.1 Overview 32

9.2 Commands 32

9.3 Processing Requirements 33
9.3.1 Online PIN 34
9.3.2 Offline PIN 34
9.3.3 Other CVM 36

9.4 PIN Pad Requirements 36

10 TERMINAL RISK MANAGEMENT 37

10.1 Overview 37

10.2 Commands 37

10.3 Processing Requirements 37

11 1ST TERMINAL ACTION ANALYSIS 39

11.1 Overview 39

11.2 Processing Requirements ... 39
11.2.1 Offline Processing Results ... 40
11.2.2 Request Application Cryptogram in 1st GENERATE AC ... 41

12 1ST CARD ACTION ANALYSIS ... 42

12.1 Overview ... 42

12.2 Commands ... 43

12.3 Processing Requirements ... 43

13 ONLINE PROCESSING ... 44

13.1 Overview ... 44

13.2 Processing Requirements ... 44

14 ISSUER AUTHENTICATION ... 46

14.1 Overview ... 46

14.2 Commands ... 46

14.3 Processing Requirements ... 46

15 2ND TERMINAL ACTION ANALYSIS ... 48

15.1 Overview ... 48

15.2 Processing Requirements ... 48
15.2.1 Advice Messages ... 49
15.2.2 Voice Referrals ... 49

16 2ND CARD ACTION ANALYSIS ... 50

16.1 Overview ... 50

16.2 Commands ... 50

16.3 Processing Requirements ... 51

17 ISSUER SCRIPT PROCESSING ... 52

17.1 Overview ... 52

17.2 Commands ... 52

17.3 Processing Requirements ... 53

17.4 Processing a Blocked Application ... 53

18 TRANSACTION COMPLETION ... 54

18.1 Overview 54

18.2 Processing Requirements 54
18.2.1 Voice referrals 54

19 PERFORMANCE REQUIREMENTS 55

20 CRYPTOGRAPHIC REQUIREMENTS 56

20.1 Unpredictable Number Generation 56

20.2 Offline Data Authentication 56

20.3 Offline PIN Encipherment 56

20.4 PIN Entry Device 56

21 ADDITIONAL PRODUCT SPECIFICS 57

21.1 Membership-Related Data Processing 57
21.1.1 Overview 57
21.1.2 Data 57
21.1.3 Processing Requirements 57

22 DATA ELEMENTS 58

22.1 Data Overview 58

22.2 Payment Systems Environment 58
22.2.1 PSE Select Response Data 58
22.2.2 PSE Directory Level Data 59

22.3 Payment Application Data 59
22.3.1 Select Response Data 59
22.3.2 Initiate Application Processing Data 61
22.3.3 Read Record Data 62
22.3.4 SDA Data 67
22.3.5 DDA / CDA Data 68
22.3.6 Chip Card PIN Encipherment Data 69
22.3.7 Terminal Risk Management Data 70

22.4 Data Elements Table 72

23 GLOSSARY 91

24 INDEX 94

List of Figures

Figure 3-1: AEIPS Transaction Flow 14

Figure 4-1: Application Selection Detail 18

Figure 5-1: Initiate Application Processing Detail 21

Figure 6-1: Read Application Data Detail 23

Figure 7-1: Offline Data Authentication Detail 25

Figure 7-2: Key Hierarchy 26

Figure 8-1: Processing Restrictions Detail 30

Figure 9-1: Cardholder Verification Detail 32

Figure 9-2: Cardholder Verification Terminal Process Flow 33

Figure 9-3: Offline PIN Terminal Process Flow 35

Figure 10-1: Terminal Risk Management Detail 37

Figure 11-1: Terminal Action Analysis Detail 39

Figure 12-1: 1st Card Action Analysis Detail 42

Figure 13-1: Online Processing Detail 44

Figure 14-1: Issuer Authentication Detail 46

Figure 15-1: 2nd Terminal Action Analysis Detail 48

Figure 16-1: 2nd Card Action Analysis Detail 50

Figure 17-1: Issuer Script Processing Detail 52

Figure 18-1: Transaction Completion Detail 54

Figure 22-1: AEIPS Data 58

List of Tables

Table 2-1: ISO Publications 11

Table 2-2: EMV Publications........ 12

Table 2-3: American Express Publications........ 12

Table 3-1: AEIPS Terminal Functionality Requirements 15

Table 3-2: AEIPS Command Terminal Support Requirements........ 16

Table 3-3: AEIPS Command Non-Specific Status Words 17

Table 11-1: Issuer Action Codes and corresponding Terminal Action Codes........ 40

Table 22-1: PSE Response Data........ 59

Table 22-2: PSE Directory Level Data 59

Table 22-3: Select Response Data 60

Table 22-4: Application Priority Indicator (API)........ 61

Table 22-5: Data Retrievable by Get Processing Options Command (GPO)........ 61

Table 22-6: Application Interchange Profile (AIP) 62

Table 22-7: Read Record Data Objects 63

Table 22-8: Application Usage Control (AUC)........ 64

Table 22-9: CDOL1 Data Objects 64

Table 22-10: CDOL2 Data Objects 65

Table 22-11: Authorization Response Code Values (Tag ‘8A’) 65

Table 22-12: Cardholder Verification Methods List 66

Table 22-13: Optional Data Objects........ 67

Table 22-14: Data used in Static Data Authentication 67

Table 22-15: Data Objects for Signing 68

Table 22-16: Mandatory Data for Dynamic Data Authentication........ 68

Table 22-17: Public key modulus lengths for which support is mandatory........ 69

Table 22-18: Static Data to be Authenticated........ 69

Table 22-19: DDOL Data Objects 69

Table 22-20: Mandatory Data for Chip Card PIN Encipherment.. 70

Table 22-21: Data Retrievable by GET DATA Command 70

Table 22-22: Terminal Verification Results (TVR) Settings 71

Table 22-23: AEIPS Data Elements Table (DET).. 73

Table 23-1: Acronyms and Abbreviations 91

1 Summary of Changes

Summary of changes from AEIPS 4.2 Specification:

- Document structure changes
  - All section numbers 1-17 incremented by 1 to 2-18
  - Summary of Changes now section 1
  - Data Elements moved from section 18 to 23
  - Table 11-1 added.
  - Table 11-1 renamed as Table 11-2
  - Cryptographic Requirements moved from section 19 to 20
  - Addition of sections: 19 Performance Requirements; 21 Additional Product Specifics; 24 Index
  - All Tables; Figures & internal links updated to match new structure
- Document functional changes – updates
  - Updates for EMV Bulletin No. 137
    - Use of CDA for both 1st & 2nd GENERATE AC is now recommended.
    - Mandatory check for presence of CA Public Key required for CDA, no CDA processing if not present.
  - Updates for EMV Bulleting No. 113
    - Table 22-22 updated to include Byte 1 bit 2 “SDA Selected”.
    - Additionally, in 7.3.2 set SDA Selected bit in TVR is SDA is performed.
  - Updates for EMV 4.2 to 4.3:
    - Despite EMV removing support for DDF entries to the PSE DDF directory, Terminals need to continue to support them for compatibility with existing cards
    - Introduction of CDA Mode to define CDA processing
    - Terminal Risk Management is always performed regardless of the AIP setting
    - DDA support in mandated in Terminals. This document also mandates CDA
- Document functional changes – new features
  - Added Membership related data processing in section 21.1, with new optional data elements (‘9F5A’ & ‘9F5B’)

    Introduction of PUT DATA command for contactless CVM list update via contact interface with tag (“9F6F”)
- Document functional changes – clarifications
  - Process overviews included within individual sections instead of separate section. Duplication removed.
  - Processing for APPLICATION UNBLOCK described
  - Handling online PIN
  - CDA processing options fully described
  - Setting TVR bits

2 Introduction

This version of the American Express AEIPS Terminal Technical Manual fully conforms to EMV v4.3 [EMV4.3i - iv]. There are two volumes within AEIPS:

- AEIPS Chip Card Specification
- AEIPS Terminal Manual (this document).

2.1 Scope

The purpose of this document is to outline the terminal functionality required to process American Express Chip Card transactions. All American Express Acquirers and Third Party Processors must ensure that the terminal performs American Express Chip Card transactions as defined in this manual.

Any functionality beyond that defined in this document must comply with [EMV4.3i – iv] (See section 2.3.2 for additional information).

This document only specifies requirements for Terminal interaction with American Express payment applications over a contact interface. Requirements for Terminals supporting contactless payments can be found in the American Express Expresspay Terminal Specification [XP-TERM].

This document is primarily a technical manual but the business requirements that the technical solutions address are also outlined.

Any terminal application intended to process an American Express Chip Card shall be certified against the requirements in this manual. Note that EMV certification is conditional but not sufficient in meeting this requirement.

2.2 Audience

This document is intended for American Express personnel involved with the implementation of payment products on Integrated Circuits or “chip”, American Express Global Network Services Partners, Chip Card application developers, Systems developers, Chip Card and Terminal vendors seeking a technical understanding of the functionality of Chip Cards and Terminals supporting AEIPS.

2.3 Reference Materials

Reference citations in this manual are shown as labels within square brackets (e.g., [ISO3166]). Full details of the references are given in this section.

Users of the information contained in these materials are solely responsible for identifying and obtaining any and all patent or other intellectual property licenses that may be needed for products or services developed in connection with these materials.

2.3.1 ISO

ISO standards may be ordered via the ISO Website at www.iso.org.

Table 2-1: ISO Publications

[ISO3166]	Codes for the representation of names and countries
[ISO4217]	Codes for the representation of currencies and funds
[ISO639]	Codes for the representation of names and languages
[ISO8583]	Financial Transaction Card Originated Messages - Interchange message specifications
[ISO7813]	Identification Cards - Financial transaction Cards
[ISO7816-4]	Identification Cards - Integrated circuit(s) Cards with contacts - Part 4: Inter-industry commands for interchange

[ISO7816-5]	Identification Cards - Integrated circuit(s) Cards with contacts -Part 5: Numbering system and registration procedure for application identifiers

2.3.2 EMV

EMV publications may be ordered from the EMV Co. Website at www.emvco.com.

Table 2-2: EMV Publications

[EMV4.3i]	EMV ICC Specification for Payment Systems, Book 1 – Application independent ICC to terminal interface requirements, version 4.3, November 2011
[EMV4.3ii]	EMV ICC Specification for Payment Systems, Book 2 – Security and key management, 4.3, November 2011
[EMV4.3iii]	EMV ICC Specification for Payment Systems, Book 3 – Application specification, version 4.3, November 2011
[EMV4.3iv]	EMV ICC Specification for Payment Systems, Book 4 – Cardholder, attendant and acquirer interface requirements, version 4.3, November 2011

2.3.3 American Express

There are a number of American Express documents that are relevant to AEIPS card Issuers and Acquirers, which can be obtained from GNSWEB, americanexpress.com/gns.

All American Express' AEIPS manuals operate within the boundaries defined in [EMV4.3i – iv].

Table 2-3: American Express Publications

[AG]	Acquirer Chip Card Implementation Guide
[ATG]	AEIPS Terminal Guide
[XP-TERM]	Expresspay Terminal Specification (ExpressPay 3.1)

2.4 Use of Terms

2.4.1 Optional, Mandatory or Conditional

American Express' philosophy is to facilitate market requirements while ensuring global interoperability. To this end, AEIPS' minimum requirements reflect the EMV mandatory items in addition to specific requirements for American Express.

American Express' minimum requirements are designated using the term "***mandatory***", "***required***", or "***must***". Participants wishing to implement parts of EMV beyond this may do so only if this manual does not state that those parts are not supported under AEIPS.

Markets can customize their programs beyond the minimum requirements through adoption of the ***optional*** functions and through proprietary processing. Proprietary processing, however, ***must not*** compromise global interoperability.

If a requirement is ***conditional***, it ***must*** meet the condition as defined in the value restrictions.

2.4.2 Use of the Term "Chip Card"

In general, the term "Chip Card" is used to represent the entity which performs the AEIPS Chip Card application functions. This acknowledges the possibility of the chip supporting multiple applications.

2.4.3 Cardholder or Cardmember?

The words Cardholder and Cardmember refer to "A person who has entered into an agreement and established a Card Account with an Issuer, or whose name is embossed on a Card".

2.5 Document Structure

This document is structured to guide the reader through the steps required to implement the AEIPS Terminal requirements.

It is assumed that technical readers are familiar with the EMV specifications [EMV4.3i – iv] and that all readers have a basic understanding of the technology. Each part of this document starts with a descriptive section. This is the suggested minimum reading for a business understanding of the document. Subsequent sections indicate the technical detail associated with the business function or requirement.

Section 3 provides an overview of a terminal transaction.

Sections 4 to 18 describe each of the transaction processing steps in detail, providing: an overview; list of commands; set of processing requirements.

Section 19 describes the performance requirements.

Section 20 describes the cryptographic requirements.

Section 21 describes the additional product functionality Terminals use to support additional American Express services.

Section 22 summarizes the Data Elements.

Section 23 contains a glossary of terms used in this document.

Section 24 is the index.

2.6 Notation

Throughout this document, the data elements that are defined in the Data Dictionary, Table 22-23, are marked in italics, e.g., *Card Verification Results*.

In the transaction flow diagrams that are used throughout this document, dashed lines around boxes are used to indicate the presence of ***optional*** functionality.

Hexadecimal numbers are represented within single quotes, e.g., ‘6A83’.

3 Transaction Overview

This section provides a general non-technical overview of the complete AEIPS transaction. It is important to understand this, since the rest of this document is structured around the transaction steps as defined in this section.

3.1 Functional Overview

All functions mentioned in this manual are performed as described in the EMV [EMV4.3i – iv]. Figure 3-1 shows the AEIPS transaction flow from the point at which a Chip Card is inserted into a Terminal to the point at which it is removed. Functions shown as dashed boxes are ***optional***.

This diagram is used throughout this manual where more detail of each function is provided.

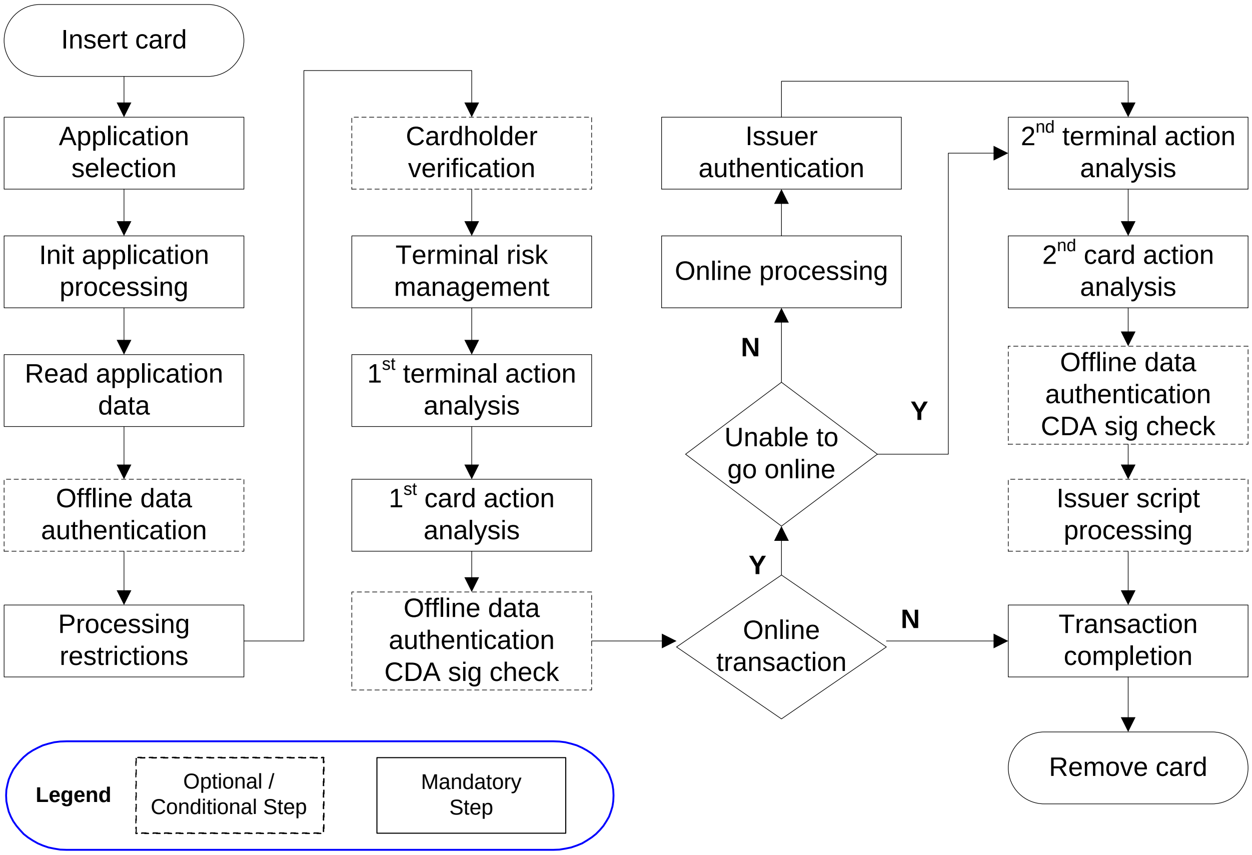

Figure 3-1: AEIPS Transaction Flow

As shown in Figure 3-1, a transaction consists of a number of processing steps which assure the AEIPS transaction. These steps are described in detail in sections 4 to 18 below.

In summary, the AEIPS transaction flow provides the means to:

- Authorize payment
- Authenticate the card
- Authenticate the transaction at the time of the transaction and for audit purposes
- Verify the Cardholder.

3.2 Dual Interface Support

A dual interface card is one that is capable of transacting over both a contact and contactless interface. The functionality ***required*** of an American Express payment application over a contact interface is defined in this manual. The functionality ***required*** of an American Express payment application over a contactless interface is defined in the Expresspay Terminal Specification [XP-TERM].

Terminal and card behavior over the contactless interface is beyond the scope of the AEIPS manuals. However, Terminals meeting this manual will successfully process dual interface cards when used on the contact interface.

3.3 Mandatory and Optional Functionality Summary

3.3.1 Functions

AEIPS Terminals ***must*** support the ***mandatory*** functions listed in Table 3-1 below. An Acquirer can then decide whether to make use of these functions or not. Unless noted, it should be assumed that ***mandatory*** parts of EMV are ***mandatory*** under AEIPS. Where AIEPS requirements differ from EMV on the presence of these functions, then this is highlighted in **bold** in Table 3-1. ***Optional*** functions may be supported at the Acquirer's discretion. ***Conditional*** functions ***must*** be supported if the associated condition is true.

Table 3-1: AEIPS Terminal Functionality Requirements

Function	Online Capable Terminals	Online Only Terminals (e.g. ATMs)	Offline Only Terminals
Application Selection • Directory Method • Explicit Selection Method • Partial Name Selection Enabled	Mandatory • Mandatory • Mandatory • Mandatory	Mandatory • Mandatory • Mandatory • Mandatory	Mandatory • Mandatory • Mandatory • Mandatory
Initiate Application Processing	Mandatory	Mandatory	Mandatory
Read Application Data	Mandatory	Mandatory	Mandatory
Offline Data Authentication • SDA • Standard DDA • Combined DDA/AC Generation • CRL checking of Issuer PKC	Mandatory • Mandatory • Mandatory • Mandatory • N/S	Optional • Optional • Optional • Optional • N/S	Mandatory • Mandatory • Mandatory • Mandatory • N/S
Processing Restrictions • Application Version Number • Application Usage Control • Effective Date Check • Expiration Date Check	Mandatory • Mandatory • Mandatory • Mandatory • Mandatory	Mandatory • Mandatory • Mandatory • Mandatory • Mandatory	Mandatory • Mandatory • Mandatory • Mandatory • Mandatory
Cardholder Verification • Signature • Online PIN • Offline PIN • No CVM	Mandatory • Mandatory • Conditional* • Optional • Conditional**	Mandatory • Mandatory • Conditional* • Optional • Conditional**	Mandatory • Mandatory • N/S • Optional • Conditional**
Terminal Risk Management • Velocity Checking • New Card Check	Mandatory • Mandatory • Mandatory	Mandatory • Mandatory • Mandatory	Mandatory • Mandatory • Mandatory
1st Terminal Action Analysis	TACs Mandatory***	TACs Mandatory***	TACs Mandatory***
1st Card Action Analysis	N/A	N/A	N/A

Function	**Online Capable Terminals**	**Online Only Terminals (e.g. ATMs)**	**Offline Only Terminals**
Online Processing • Online Capability • Issuer Authentication	Mandatory	Mandatory	N/S
2nd Terminal Action Analysis	Mandatory	Mandatory	Mandatory
2nd Card Action Analysis	N/A	N/A	N/A
Issuer Script Processing ■ Secure Messaging	**Mandatory**	**Mandatory**	N/S
Transaction Completion	Mandatory	Mandatory	Mandatory

* Online PIN is mandatory for cash advance transactions.

** No CVM is ***mandatory*** for CATs

*** It is ***mandatory*** that TACs are present.

3.3.2 Commands

The table below indicates the command requirements for an AEIPS-compliant Terminal to support the Chip Card commands defined in [EMV4.3iii].

Table 3-2: AEIPS Command Terminal Support Requirements

Command	**AEIPS Terminal Support**
EXTERNAL AUTHENTICATE	Mandatory
GENERATE AC	Mandatory
GET CHALLENGE	Mandatory
GET DATA	Mandatory
GET PROCESSING OPTIONS	Mandatory
GET RESPONSE	Mandatory
INTERNAL AUTHENTICATE	Mandatory
READ RECORD	Mandatory
SELECT	Mandatory
VERIFY	Mandatory

3.3.3 AEIPS Command Non-Specific Status Words

The table below indicates the status word responses that an AEIPS-compliant card may generate in response to errors processing commands. Additional status words representing particular errors specific to a command can be found in the appropriate section of the document. The order column indicates the order in which error checking will be performed by the card.

Table 3-3: AEIPS Command Non-Specific Status Words

Order	Error Condition	Status Word
1	When any command is attempted with an CLA byte not equal to one of ‘00’, ‘04’, ‘80’, ‘84’.	6E00
2	When a command is attempted with an INS byte not equal to one of: ‘A4’, ‘A8’, ‘B2’, ‘CA’, ‘20’, ‘88’, ‘AE’, ‘82’, ‘1E’, ‘24’, ‘DA’, ‘18’.	6D00
3	When a supported card command completes processing without error	9000

4 Application Selection

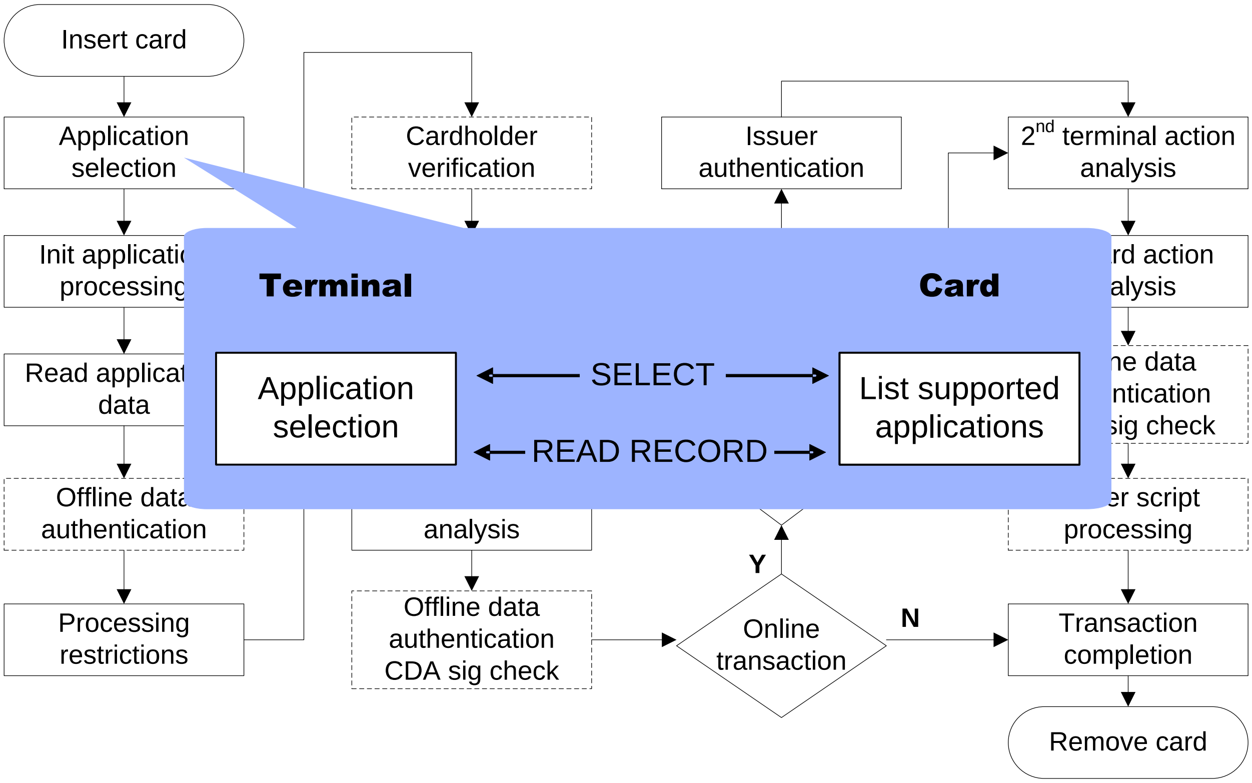

Figure 4-1: Application Selection Detail

4.1 Overview

When an AEIPS Chip Card is presented to a Terminal, the Terminal determines, and ***optionally*** displays, a list of applications supported by both Chip Card and Terminal. In the case where the list is displayed, the Cardholder selects the desired application from the available list.

When the Terminal does not support Cardholder selection the terminal selects the application according its priority.

During Application Selection, the Chip Card and Terminal determine which of the applications that are supported by both will be used to conduct the transaction. Two steps are performed:

- Build the candidate list: The Terminal builds a list of mutually supported applications.
- Application selection: A single application from the candidate list is identified and selected for the following transaction.

4.2 Commands

- SELECT
- READ RECORD

To support Application Selection as described in [EMV4.3i] Sections 11.2 and 11.3, the Terminal ***must*** support the READ RECORD and the SELECT commands.

4.3 Processing Requirements

Card Application selection consists of a number of stages:

- Card Insertion and Power Up Sequence
- Answer to Reset
- Application Selection – Building the Candidate List
- Application Selection – Choosing the Required Application.

4.3.1 Chip Card Insertion and Power Up Sequence

Terminals ***must*** be fully compliant to the requirements detailed in [EMV4.3i] *Part I – Electromechanical Characteristics and Logical Interface and Transmission Protocols*.

4.3.2 Answer to Reset

The Chip Card reader ***must*** be fully compliant with the requirements of [EMV4.3i] *Part II – Electromechanical Characteristics and Logical Interface and Transmission Protocols.* This details the electromechanical characteristics and transmission protocols to be used for communication between Chip Card and Terminal.

4.3.2.1 Protocol Support

Two transmission protocols are defined in the EMV Specifications:

- T = 0 – Character-oriented asynchronous half-duplex transmission protocol
- T = 1 – Block-oriented asynchronous half-duplex transmission protocol.

The Terminal ***must*** be capable of supporting both protocols.

If a Chip Card does not support a protocol which is supported by the Terminal, i.e., other than T=0 or T=1, fallback to magnetic stripe ***must*** apply.

4.3.3 Application Selection – Building the Candidate List

Applications are identified by *Application Identifiers (AIDs)*. *AIDs* are intended to identify a Chip Card product or service provider, i.e., American Express Charge Card, American Express Credit Card, etc.

The following EMV documents detail the Terminal requirements for the support of the EMV Application Selection process:

- [EMV4.3i] Section 12
- [EMV4.3iv] Section 11.3.

Note that EMV4.3 removes other DDF entries from the PSE DDF directory. However, terminals ***must*** continue to process application selection of PSE with DDF entries in accordance with previous versions of EMV and as detailed in [ISO7816-4] until the cards are replaced.

EMV specifies two methods for identifying the candidate list of applications for selection:

- Using a Terminal held list of supported AIDs, as described in [EMV4.3i] Section 12.3.3
- Using the Payment Systems Environment (PSE), as described in [EMV4.3i] Section 12.3.2.

Terminals compliant with this manual ***must*** support both methods. If the PSE is present on the card then the PSE selection method ***must*** be attempted first.

If either the card does not have a PSE, or PSE processing does not identify a suitable application, the Terminal ***must*** use a list of AIDs it supports to build the candidate list.

Additionally, all AEIPS compliant terminals ***must*** support the use of partial name selection, as described in [EMV4.3i] Section 11.3.5.

If there are no applications supported by both the Chip Card and Terminal, the transaction ***must*** be terminated.

The Registered Application Provider Identifier (RID) assigned to American Express is ‘A000000025’.

4.3.4 Application Selection – Choosing the Required Application

There are three scenarios depending on the display capabilities and environment of the terminal:

- **Terminal supports Cardholder selection** - if the Terminal supports Cardholder selection, the Cardholder ***must*** be presented with an application list in priority order. If the Cardholder does not select an application, the transaction ***must*** be terminated.
- **Terminal supports Cardholder confirmation** - if the Terminal supports Cardholder confirmation, then it will select the highest priority application and ***must*** ask for Cardholder confirmation. If the Cardholder confirms, the application ***must*** be selected. Otherwise the Terminal ***must*** select the next highest priority application, until the Cardholder confirms, or no further applications exist. If the Cardholder does not select an application, the transaction ***must*** be terminated.
- **Terminal does not support Cardholder selection or confirmation** - if the Terminal does not support application selection or confirmation by the Cardholder, the Terminal ***must*** select the highest priority application that does not require Cardholder confirmation.

The application priority is indicated by the value of the *Application Priority Indicator* read from the Chip Card.

The *Application Priority Indicator* also defines whether a particular application requires specific Cardholder confirmation before use in a transaction. Operational design and Terminal location should take this into account if a Terminal is going to support such applications.

If as a result of application selection a list is presented to the Cardholder, it ***must*** be in priority sequence, with the highest priority application listed first.

If there is no priority sequence specified in the card, the list should be in the order in which the applications were encountered in the card, unless the terminal has its own preferred order. The same applies where duplicate priorities are assigned to multiple applications or individual entries are missing the Application Priority Indicator i.e. the terminal may use its own preferred order or display the duplicate priority or non-prioritized applications in the order encountered in the card.

If there is only one AEIPS application supported by both the Chip Card and Terminal, the Terminal may select it automatically without involving the Cardholder if the payment application does not require cardholder confirmation

If there is only one AEIPS application supported by both the Chip Card and Terminal which requires cardholder confirmation, then explicit Cardholder selection ***must*** ensue.

Once the Terminal has identified the application to be used for the transaction, it ***must*** be selected by the Terminal using the SELECT command, as defined in [EMV4.3i] Section 11.3 SELECT Command-Response APDUs.

5 Initiate Application Processing

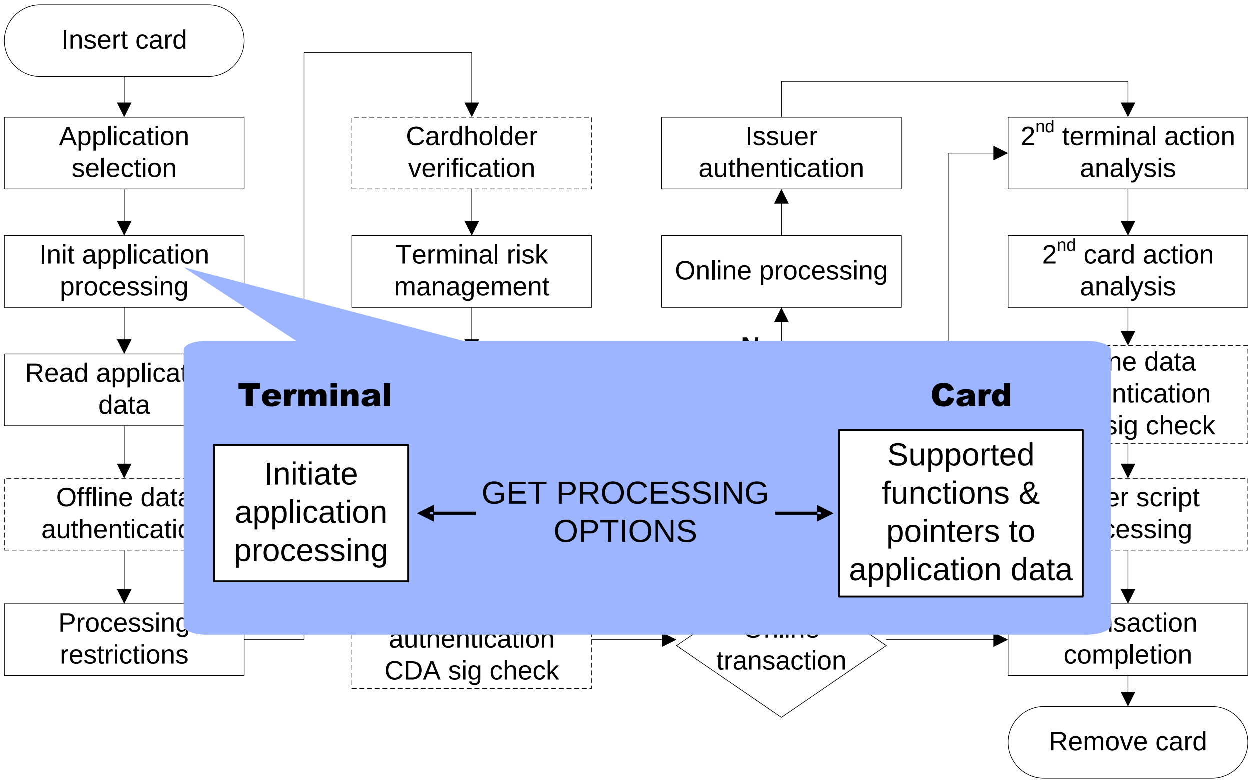

Figure 5-1: Initiate Application Processing Detail

5.1 Overview

If an AEIPS application is selected, the Terminal requests that the Chip Card presents the location of the data to be used for the current transaction and the functions supported.

The GET PROCESSING OPTIONS command signals the Chip Card to return the *Application File Locator (AFL)* and *Application Interchange Profile* (*AIP*).

The *AFL* is a list of parameters identifying the files and records to be read from the Chip Card used in processing the transaction. The *AIP* indicates the capabilities of the Chip Card to support specific functions of the application to be taken into consideration by the Terminal when determining how to process the transaction.

5.2 Commands

- GET PROCESSING OPTIONS

To support Initiate Application Processing, the Terminal ***must*** support the GET PROCESSING OPTIONS command as defined in [EMV4.3iii] Section 6.5.8.

5.3 Processing Requirements

The Terminal ***must*** determine whether the ***optional*** *Processing Data Object List (PDOL)* was supplied by the Chip Card application in response to the application selection.

If the *PDOL* is used, the Terminal ***must*** format the GET PROCESSING OPTIONS command to include any data elements requested in the *PDOL* to be sent to the Chip Card with this command.

If the *PDOL* is not present, the Terminal ***must*** format the GET PROCESSING OPTIONS command with the command data field of ‘8300’.

The Terminal ***must*** format the GET PROCESSING OPTIONS command according to [EMV4.3iii] Section 6.5.8.

During Application Initiation, the Terminal signals the Chip Card that processing of the transaction is beginning. Initiate Application Processing ***must*** be performed as described in [EMV4.3iii] Section 10.1, and [EMV4.3iv] Section 6.3.1 and store the *AFL* and *AIP* returned from the Chip Card.

If the response from the Chip Card returns SW1 SW2 = ‘6985’ indicating that ‘Conditions of use are not satisfied’, the Terminal ***must*** remove the current application from the list of mutually supported applications (the candidate list) and return to Application Selection (See Section 4).

If the response from the Chip Card does not contain both the *AFL* and *AIP* then the Terminal ***must*** remove the current application from the list of mutually supported applications (the candidate list) and return to Application Selection (See Section 4).

If the response from the Chip Card returns the *AFL* and *AIP*, the Terminal ***must*** proceed to Read Application Data (See Section 6).

6 Read Application Data

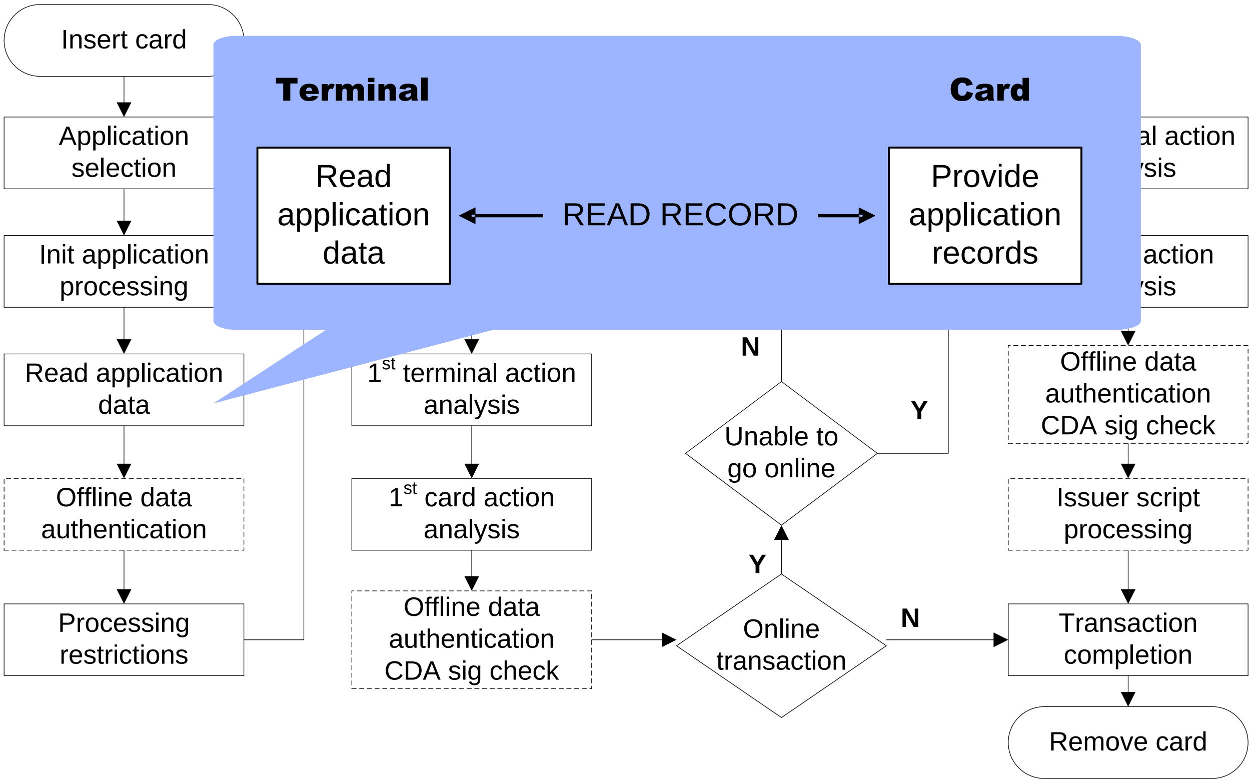

Figure 6-1: Read Application Data Detail

6.1 Overview

The Terminal reads the data from the location presented by the Chip Card *AFL*.

The Terminal reads any Chip Card data necessary for completing the transaction using the READ RECORD command. The *AFL* is a list identifying the files and records that must be used in the processing of a transaction. The files that are read may be used for application purposes or as authentication data used during Offline Data Authentication (See Section 7).

6.2 Commands

- READ RECORD

AEIPS compliant Terminals ***must*** support the READ RECORD command as described in [EMV4.3iii] Section 6.5.11.

6.3 Processing Requirements

The Terminal ***must*** read all data records specified in the *AFL*.

It is ***mandatory*** that the READ RECORD command be performed as defined in [EMV4.3i] Section 11.2.

All data read successfully from the Chip Card ***must*** be stored by the Terminal and used when required during the transaction. If a processing error occurs during this read record phase, the transaction ***must*** be aborted.

It is not the Terminal's responsibility to ensure the integrity of the data read from the Chip Card unless it is a specific requirement of the EMV specifications. As long as the data retrieved within a read record command correctly breaks down into valid Tag/Length/Value (TLV) data elements, the Terminal can assume it is valid, and the integrity of the data element placed in a Chip Card is the responsibility of the Issuer.

Terminal vendors ***must*** ensure that an invalid data element value does not cause the Terminal to become unusable or lock up.

Data validation (missing or erroneous data on the Chip Card) is detailed in [EMV4.3iii] Section 7.5, in particular the *Terminal Verification Results* (TVR) byte 1, bit 6 ***must*** be set according to [EMV4.3iii] Table 31.

7 Offline Data Authentication

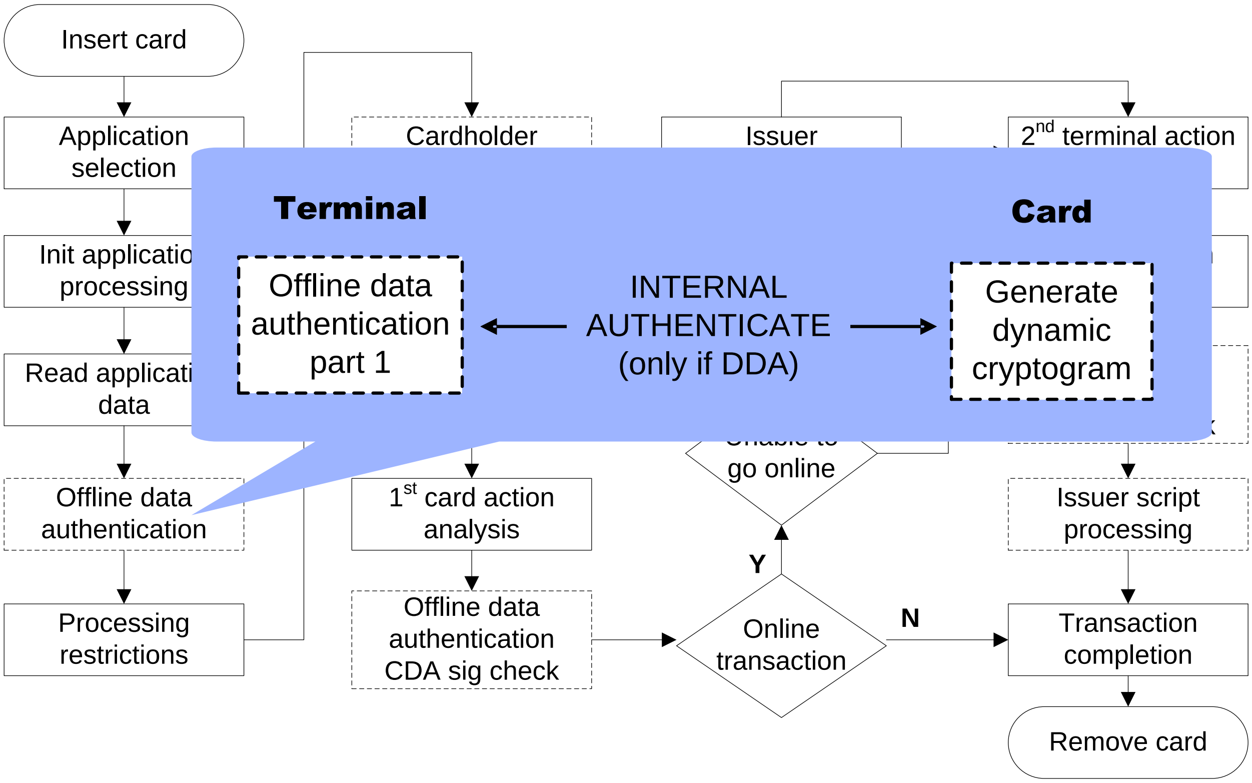

Figure 7-1: Offline Data Authentication Detail

7.1 Overview

Offline Data Authentication is a mechanism intended to prove that certain significant card data elements have not been altered after the Chip Card was issued. “Static” data authentication proves that data is not counterfeit and “dynamic” data authentication proves that the data is not cloned. The three forms of data authentication are:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA/Application Cryptogram Generation (CDA).

The Terminal determines whether it should authenticate the Chip Card offline using either static or dynamic data authentication based upon the Chip Card support for these methods.

Offline Data Authentication results are used when the Chip Card and Terminal decide whether to approve the transaction offline, go online for approval or to decline the transaction.

Offline Data Authentication uses Public Key Cryptography. Figure 7-2 shows the one-to-one and the one-to-many relationships in the American Express Public Key Scheme. At the top of the trust tree there is the American Express EMV Certificate Authority (CA). Directly under this, each issuing Participant has a CA and each issues many Chip Cards. Each AEIPS-compliant Chip Card holds the Issuer’s Public Key Certificate which is signed by an American Express EMV CA private key. Each payment application on an AEIPS-compliant Chip Card may hold an Application DDA Private Key and Public Key Certificate which is signed by an Issuer CA Private Key. For the cryptographic scheme to work, each Terminal need only hold the set of American Express EMV CA Public Keys.

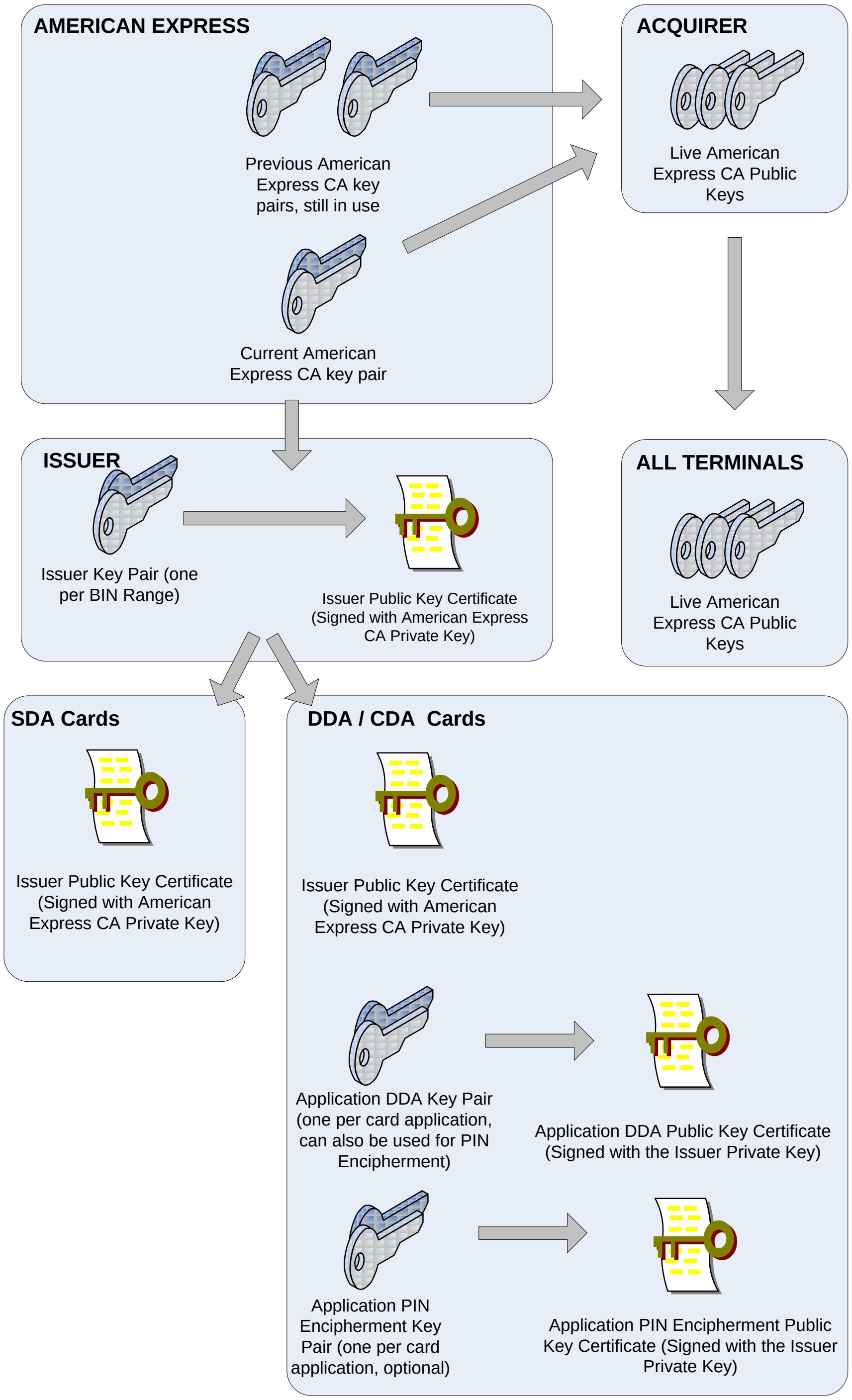
AMERICAN EXPRESS
Previous American Express CA key pairs, still in use
Current American Express CA key pair
ACQUIRER
Live American Express CA Public Keys
ISSUER
Issuer Key Pair (one per BIN Range)
Issuer Public Key Certificate (Signed with American Express CA Private Key)
ALL TERMINALS
Live American Express CA Public Keys
SDA Cards
Issuer Public Key Certificate (Signed with American Express CA Private Key)
DDA / CDA Cards
Issuer Public Key Certificate (Signed with American Express CA Private Key)
Application DDA Key Pair (one per card application, can also be used for PIN Encipherment)
Application DDA Public Key Certificate (Signed with the Issuer Private Key)
Application PIN Encipherment Key Pair (one per card application, optional)
Application PIN Encipherment Public Key Certificate (Signed with the Issuer Private Key)

Figure 7-2: Key Hierarchy

Note: The Application DDA keys may also be used for offline PIN encipherment during cardholder verification. Alternatively, a payment application may include a separate Application PIN encipherment Public and Private Key if this function is supported, and is shown in the figure. Section 9 describes cardholder verification.

7.1.1 Static Data Authentication (SDA)

SDA validates a fixed cryptographic signature over data elements held within the Chip Card to assure that this data has not been altered since Chip Card personalization. The Terminal uses the Issuer Public Key retrieved from the Chip Card to decrypt the data from the Chip Card and make sure that the hash obtained in this way matches a hash of the actual data objects retrieved from the Chip Card. If these hashes do not match, then offline SDA fails.

During SDA, the Chip Card is passive and the Terminal is active. The Chip Card provides the data to be validated but the terminal carries out all the computation.

7.1.2 Dynamic Data Authentication (DDA)

DDA is an offline authentication technique in which the Chip Card and the Terminal are both active and capable of executing a Public/Private Key algorithm. DDA validates not only that the Chip Card data has not been altered but also that the data is being read from a genuine card and is not a copy.

As part of DDA processing the Terminal verifies the Chip Card static data has not been altered in a similar manner to SDA. In addition, the Terminal validates that the card is genuine in a separate process by requesting that the Chip Card generates a cryptogram using dynamic (transaction unique) data from the Chip Card and Terminal and a Chip Card Application DDA Private Key. The Terminal decrypts this dynamic signature using the Chip Card Application DDA Public Key recovered from Chip Card data. A match of the decrypted data to a hash of the original data verifies that the Chip Card is not a counterfeit.

7.1.3 Combined DDA / Application Cryptogram Generation (CDA)

CDA was introduced to EMV to enable transactions to be performed more efficiently and securely by directly linking the Application Cryptogram used in authorization and settlement with the offline authentication process. CDA is an offline authentication mechanism that uses a similar technique to DDA, but combines the generation of the offline authentication signature with the generation of the Application Cryptogram. This means that the Terminal does not perform offline data authentication processing as a separate process but as part of the processing of the Application Cryptogram produced by the card as a result of Card Action Analysis (Sections 12 and 16).

7.2 Commands

- READ RECORD
- INTERNAL AUTHENTICATE (DDA Only)

The data elements used for Offline Data Authentication are read from the Chip Card by the Terminal using the READ RECORD command during the “Read Application Data” phase of the transaction. If supported, the INTERNAL AUTHENTICATE command ***must*** be performed as specified in [EMV4.3iii] Section 6.5.9 INTERNAL AUTHENTICATE Command-Response APDUs.

Only one INTERNAL AUTHENTICATE command ***must*** be supported per transaction.

7.3 Processing Requirements

AEIPS ***requires*** that all Terminals are capable of performing Offline Data Authentication except Terminals operating in certain 'online only' environments, for example ATMs.

Offline Data Authentication can take three forms as described in the EMV 4.3 specifications. AEIPS-compliant Terminals ***must*** support:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA/Application Cryptogram Generation (CDA).

Offline Data Authentication ***must*** be performed as described in [EMV4.3ii] Sections 5 and 6, and [EMV4.3iii] Section 10.3. TVR bits affected include byte 1, bits 8, 7, 4 and 3. If Offline Data Authentication is not performed, then TVR byte 1, bit 8 ***must*** be set to "1".

The Terminal ***must*** determine Chip Card authentication using SDA, DDA or CDA based on the Chip Card support for these methods as indicated in the *AIP* of the Chip Card.

When Offline Data Authentication is to be performed, CDA has the highest priority and if the Chip Card supports it, then CDA ***must*** be performed. If the card only supports DDA and/or SDA then DDA ***must*** be attempted. If the Chip Card does not support either type of dynamic data authentication, but does support Static Data Authentication (SDA), then SDA ***must*** be performed.

Any Terminal that has the ability to complete a transaction offline (i.e., without positive online authorization from the Issuer of the Chip Card) ***must*** support and perform Offline Data Authentication (subject to the Chip Card indicating Offline Data Authentication is supported in the *AIP*).

EMV optionally supports the use of a Certificate Revocation List (CRL) to enable the listing of Issuer Public Key Certificates that a Payment Scheme has revoked. American Express ***does not support*** the use of CRLs for this purpose at this time.

7.3.1 American Express Scheme CA Keys

In order that Offline Data Authentication can be performed by a Terminal, the Terminal ***must*** be configured with the necessary American Express Certificate Authority (CA) Public Keys.

American Express will distribute the American Express CA Public Keys (CAPKs) to Acquirers of American Express Chip Card transactions. The Acquirers are responsible for the distribution of the American Express CAPKs to all Terminals that support Offline Data Authentication.

Terminals ***must*** be able to store and use a minimum of six American Express CAPKs and associated data, permitting all keys to be available for use during the processing of a Chip Card transaction.

The CAPKs, their related data elements that a Terminal must hold along with details of the format in which the CAPKs are distributed by American Express are shown in the American Express Terminal Guide [ATG].

7.3.2 Static Data Authentication (SDA)

If Static Data Authentication is to be performed, then the Terminal ***must***:

- Check that the CAPK identified by the Card is configured.
  - If the CAPK is not present or is invalid, then SDA fails and the Terminal ***must*** set the TVR byte 1 bit 7 to "1" (SDA Failed).
- If Static Data Authentication is to be performed then this ***must*** be performed as described in [EMV4.3ii] Sections 5 and 6, and [EMV4.3iii] Section 10.3.
  - The Terminal ***must*** set the TVR byte 1 bit 2 "SDA selected" to "1".
- During SDA the Terminal will validate the Signed Static Application Data read from the Chip Card. If SDA fails, the Terminal ***must*** set the TVR byte 1, bit 7 "SDA Failed" bit to "1".

7.3.3 Dynamic Data Authentication (DDA)

If Standard Dynamic Data Authentication, as described in [EMV4.3ii] Section 6.5, is to be performed, the INTERNAL AUTHENTICATE command ***must*** be issued to the Chip Card as described in [EMV4.3iii] Section 6.5.9 Command-Response APDUs.

The INTERNAL AUTHENTICATE Command ***must*** include a concatenation of the data elements identified in the *Dynamic Authentication Data Object List (DDOL)* read from the Chip Card, or in the event that the *DDOL* is not present in the Chip Card the Terminal ***must*** use the Default *DDOL* (tag '9F37') present in the Terminal. In all cases the *DDOL* ***must*** contain the *Unpredictable Number* (tag '9F37') otherwise DDA is considered by the Terminal to have failed.

If DDA is to be performed, then the Terminal ***must*** check that the CAPK identified by the Card is configured.

- If the CAPK is not present or is invalid, then DDA fails and the Terminal ***must*** set the TVR byte 1 bit 4 to "1" (DDA Failed).

During DDA the Terminal ***must*** validate the *Signed Dynamic Application Data* returned by the card in the response to the INTERNAL AUTHENTICATE Command.

If DDA fails the Terminal ***must*** set the TVR byte 1, bit 4 "DDA Failed" to "1".

7.3.4 Combined DDA/AC Generation (CDA)

If CDA is to be performed, the INTERNAL AUTHENTICATE Command is not issued to the Chip Card. Instead, CDA can be requested by a Terminal in the following circumstances:

- When requesting a TC as part of 1st GENERATE AC
- When requesting an ARQC as part of 1st GENERATE AC
- When requesting a TC as part of 2nd GENERATE AC.

Terminals supporting Offline Data Authentication have 4 operating modes for when requesting an online cryptogram from the Chip Card and processing an approved online authorization:

- CDA to be requested on 1st and 2nd GENERATE AC
- CDA to be requested on 1st but not the 2nd GENERATE AC
- CDA is not requested on 1st or 2nd GENERATE AC
- CDA to be requested only on the 2nd GENERATE AC.

Terminals can be configured to support any one of the modes for AEIPS transactions. American Express recommends that terminals request CDA on both the 1st and 2nd GENERATE AC, which corresponds to CDA Mode 1 in [EMV4.3ii] Table 30.

If requested, CDA processing is performed following Card Action Analysis and is described in Sections 12 and 16.

If CDA is to be performed, either following the 1st and / or 2nd GENERATE AC, the Terminal ***must*** check that the CAPK identified by the card is configured.

- If the CAPK is not present then CDA ***shall*** be considered to have failed, CDA ***must not*** be requested in the GENAC and the Terminal ***must*** set the TVR byte 1, bit 3 "CDA Failed" to "1".

8 Processing Restrictions

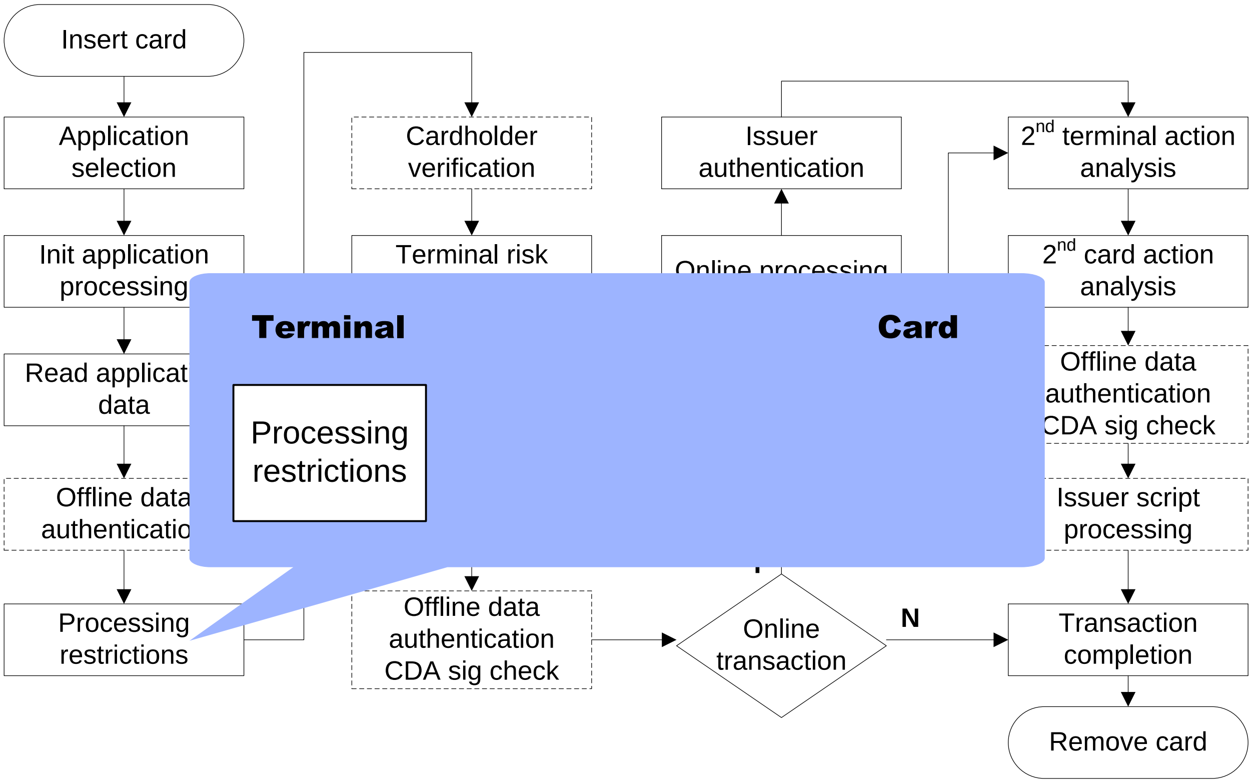

Figure 8-1: Processing Restrictions Detail

8.1 Overview

The Terminal performs a number of checks to see whether the transaction should be allowed. Parameters that can effect this decision include the effective and expiration date for the Chip Card, whether the application versions of the Chip Card and Terminal match, and whether any *Application Usage Control* restrictions are in effect. An Issuer may use *Application Usage Controls* to restrict a Chip Card's use for cash, goods or services.

The Terminal uses the data gathered from the Chip Card during Read Application Data (See Section 6) to ascertain the particular restrictions under which this transaction can be carried out.

8.2 Processing Requirements

The Terminal ***must*** perform Processing Restrictions, as defined in [EMV4.3iii] Section 10.4 and [EMV4.3iv] Sections 6.3.3, to see whether the transaction should be allowed.

Processing Restrictions cover the following ***mandatory*** checks to be performed by the Terminal:

- Comparison of the Chip Card Application Version Number, if present in the Chip Card, to a Terminal-resident Application Version Number. The Terminal ***must*** store an Application Version Number for each Application Identifier (AID) supported by the Terminal. If the Chip Card Application Version Number and Terminal-resident Application Version Number are not the same, then the Terminal ***must*** set the TVR byte 2 bit 8 to "1" as described in [EMV4.3iii] Section 10.4.1.
- Application Usage Control - This is used to determine if any geographical or transaction type restrictions have been imposed on the Chip Card product, e.g., it may be used to restrict a Chip Card's use for domestic or international cash, or goods and services:
  - Domestic Usage Check - If the *Issuer Country Code* read from the Chip Card is equal to the *Terminal Country Code,* the transaction is defined as 'Domestic'. The Terminal checks that the transaction type (e.g., Cash, Goods or Services) for the transaction being processed is

permitted in a ‘Domestic’ environment according to the Chip Card’s *Application Usage Control (AUC).*

- International Usage Check - If the *Issuer Country Code* read from the Chip Card is not equal to the *Terminal Country Code,* the transaction is defined as ‘International’. The Terminal checks that the transaction type for the transaction being processed is permitted in an ‘International’ environment according to the Chip Card’s *Application Usage Control (AUC).*
- Transaction Environment Check – If the Terminal is an ATM the Terminal checks that the Chip Card’s *AUC* has the bit “Valid for use at an ATM” set to 1. If the Terminal is other than an ATM (e.g., POS), the Terminal must verify that the Chip Card’s *AUC* has the bit “Valid at Terminals other than an ATM” set to “1”.

If any of the above checks fail, the Terminal ***must*** set byte 2 bit 5 of the TVR to “1” indicating that the “Requested Service is not Allowed for Card Product”.

- *Effective* and *Expiration Date* Checking – These checks ensure that the application is not pre-valid and not expired. If the transaction date is prior to the *Application Effective Date*, the Terminal ***must*** set the *TVR* byte 2 bit 6 (Application not effective yet) to “1”. If the transaction date is past the *Application Expiration Date*, the Terminal ***must*** set the *TVR* byte 2 bit 7 (Expired application date) to “1”.

The outcomes of the above checks are evaluated against a set of *Issuer Action Codes* and *Terminal Action Codes* resident in the Chip Card and Terminal respectively during Terminal Action Analysis (See Section 11).

9 Cardholder Verification

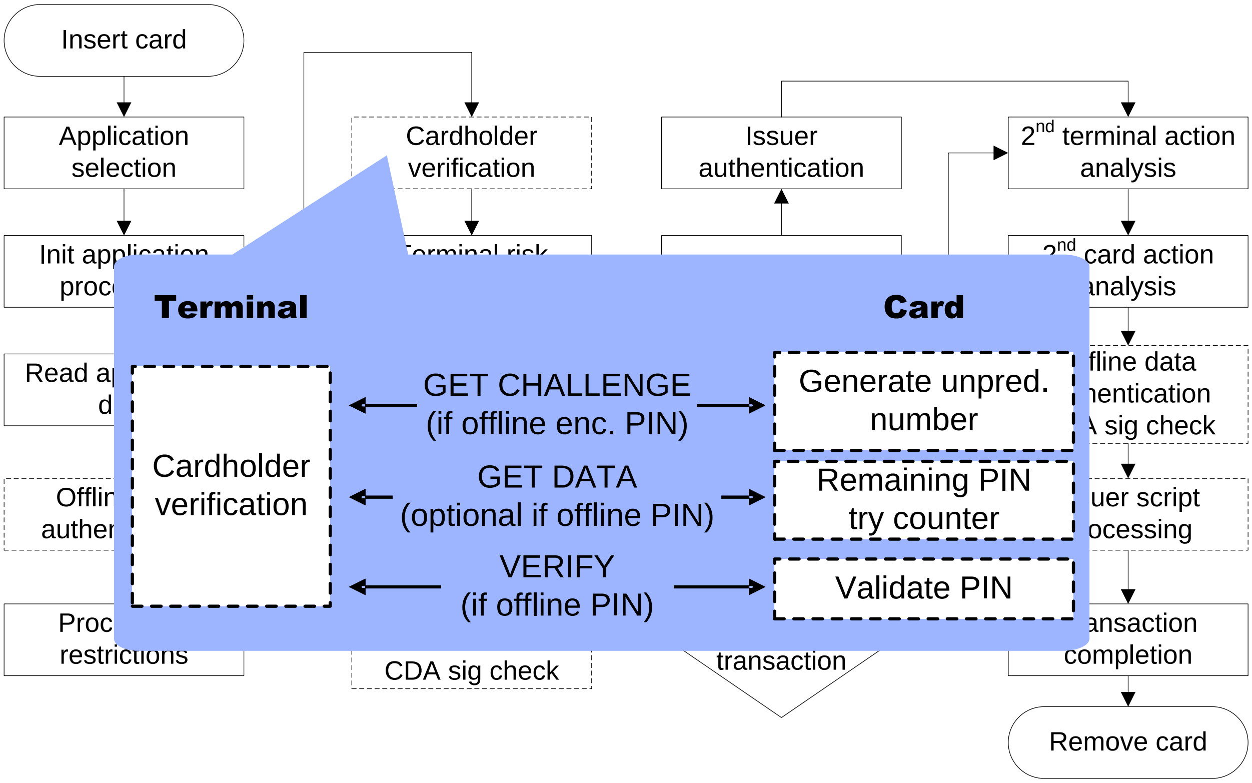

Figure 9-1: Cardholder Verification Detail

9.1 Overview

Cardholder Verification is used to determine that the Cardholder is legitimate and that the Chip Card has not been lost or stolen.

The Chip Card's *Cardholder Verification Method (CVM) List* is used by the Terminal to identify the highest priority CVM that both the Chip Card and Terminal support. The Terminal reads this list, and when a match of the conditions required by the Chip Card and the methods supported by the Terminal is found, that CVM method is selected.

9.2 Commands

- GET DATA
- GET CHALLENGE
- VERIFY

If the Chip Card and Terminal support offline PIN the Terminal ***must*** use the GET DATA command to read the *Remaining PIN Try Counter* as defined in [EMV4.3iii] Section 6.5.7 GET DATA Command-Response APDUs. This enables the Terminal to identify a blocked PIN without having to issue a VERIFY command.

For offline PIN processing, if supported, the Terminal application ***must*** support the VERIFY command, as defined in [EMV4.3iii] Section 6.5.12. If enciphered offline PIN is supported, the Terminal application ***must*** also support the GET CHALLENGE command, as defined in [EMV4.3iii] Section 6.5.6.

9.3 Processing Requirements

Cardholder Verification ***must*** be supported by the Terminal as defined in [EMV4.3iii] Section 10.5 and [EMV4.3iv] Section 6.3.4.

CVM Processing is shown in Figure 9-2 and described in the following.

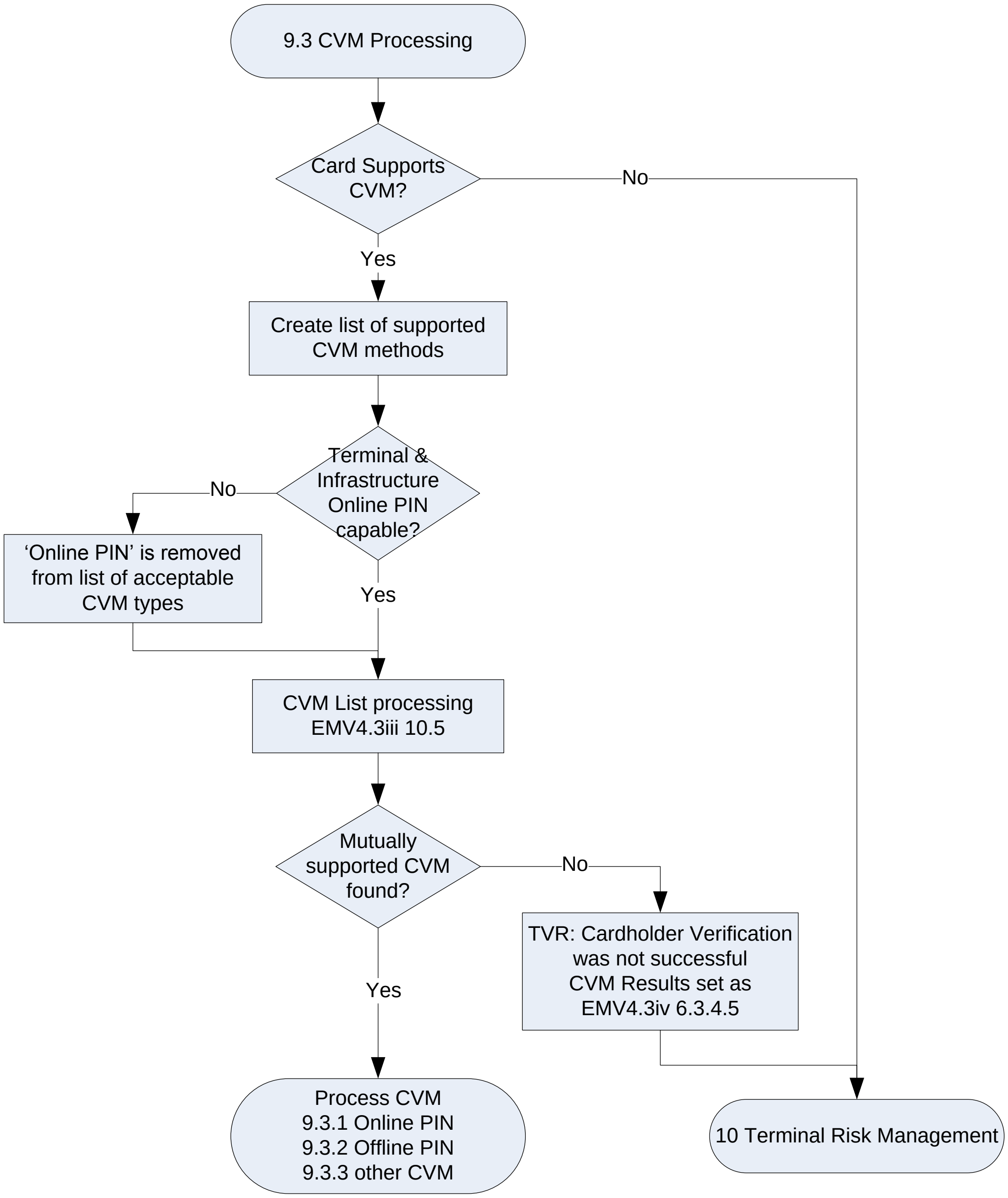
9.3 CVM Processing
Card Supports CVM?
No
Yes
Create list of supported CVM methods
Terminal & Infrastructure Online PIN capable?
No
'Online PIN' is removed from list of acceptable CVM types
Yes
CVM List processing EMV4.3iii 10.5
Mutually supported CVM found?
No
TVR: Cardholder Verification was not successful CVM Results set as EMV4.3iv 6.3.4.5
Yes
Process CVM 9.3.1 Online PIN 9.3.2 Offline PIN 9.3.3 other CVM
10 Terminal Risk Management

Figure 9-2: Cardholder Verification Terminal Process Flow

- If the *AIP* returned by the card in response to the GET PROCESSING OPTIONS command indicates that Cardholder Verification is supported, the Terminal ***must*** perform Cardholder Verification processing as defined in [EMV4.3iii] Section 10.5 and [EMV4.3iv] Section 6.3.4. In particular, processing continues as follows:
  - The *Cardholder Verification Method (CVM) List* present on the Chip Card drives the Cardholder Verification processing requirements. A Terminal ***must not*** attempt to use any CVM unless it is indicated to do so by the *Cardholder Verification Method (CVM) List.*

  - If either the Terminal or the associated acquiring infrastructure for the payment system Card being processed does not support the Cardholder Verification Method of Online PIN, then the Terminal ***must not*** include 'Online PIN' as one of its supported methods (see Section 9.3.1).
  - The Terminal ***must*** process the *Cardholder Verification Method (CVM) List* as defined in [EMV4.3iii] Section 10.5.5. Additionally, the Terminal must perform the operations described for individual CVMs as described in the following Sections 9.3.2 and 9.3.3.
  - If the result of CVM processing is a CVM fail then the Terminal ***must*** set the TVR byte 3 bit 8 (Cardholder verification was not successful) to "1" as per [EMV4.3iii] Section 10.5 and CVM Results as [EMV4.3iv] Section 6.3.4.5.
- Else *AIP* indicates Cardholder Verification is not supported and processing continues with Terminal Risk Management Section 10.

9.3.1 Online PIN

If the CVM for the transaction is Online PIN, the Terminal ***must*** prompt for PIN irrespective of the status of the Chip Card's Offline PIN (i.e., including the case where the Chip Card's Offline PIN Try Limit is exceeded). Furthermore, the terminal ***must*** perform an online transaction with the Issuer to complete CVM checking and hence ***must not*** request an offline approval during Terminal Action Analysis (section 11).

If the Online PIN is entered and accepted by the Terminal, the Terminal ***must*** set the *Terminal Verification Results (TVR)* byte 3 bit 3 ("Online PIN Entered") to "1", and the result of the CVM is considered to be successful.

If a terminal is to support Online PIN then both the Point of Sale Terminal and the acquiring infrastructure (message protocols, etc.) ***must*** be able to support inclusion of the Online PIN in the authorization request sent to American Express. The terminal and the acquiring infrastructure ***must*** be certified for Online PIN before the Terminal is considered capable of supporting Online PIN as a CVM.

9.3.2 Offline PIN

Offline PIN processing proceeds as shown in Figure 9-3.

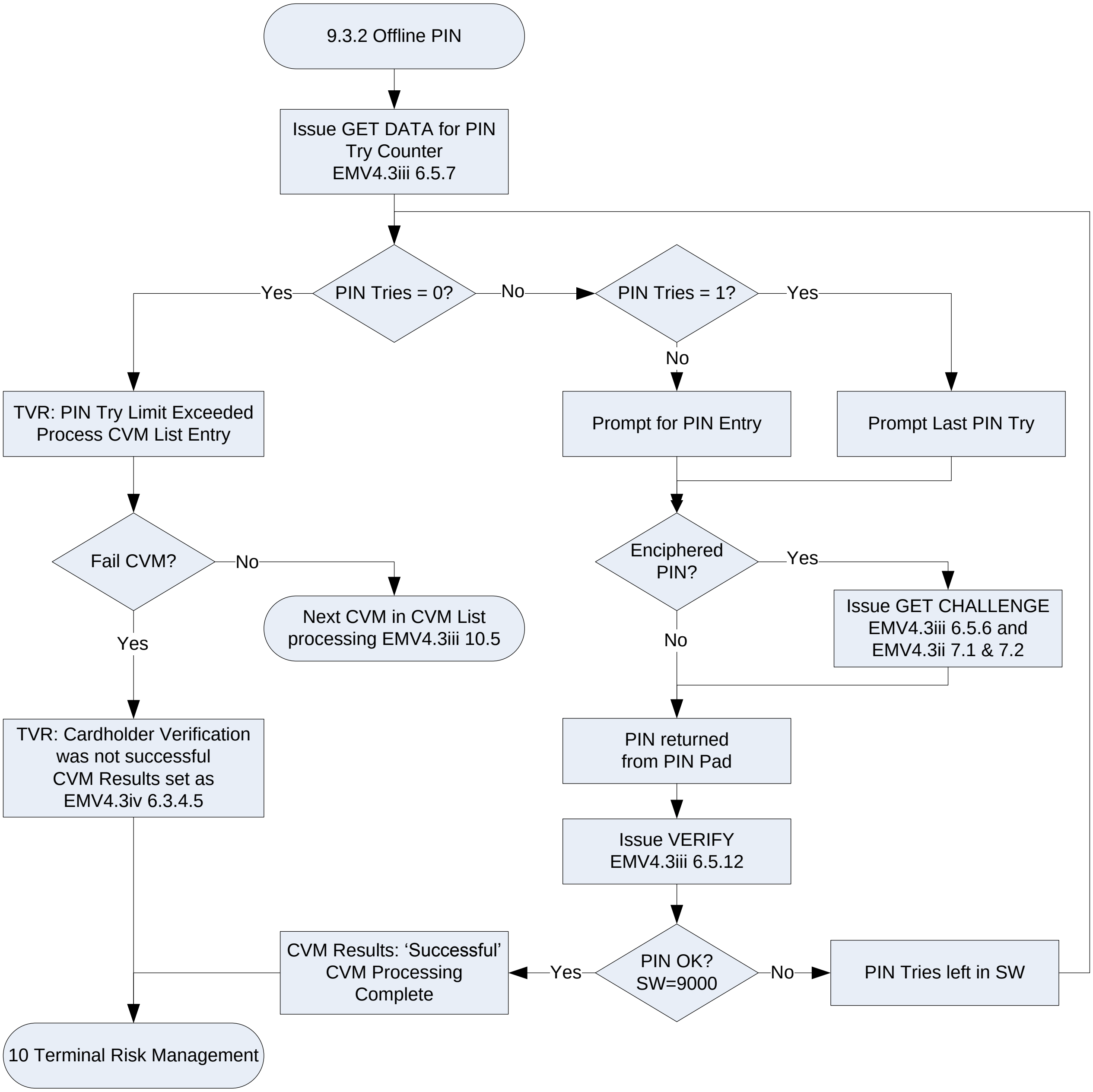
9.3.2 Offline PIN
Issue GET DATA for PIN Try Counter EMV4.3iii 6.5.7
PIN Tries = 0?
Yes
No
PIN Tries = 1?
Yes
No
TVR: PIN Try Limit Exceeded Process CVM List Entry
Prompt for PIN Entry
Prompt Last PIN Try
Fail CVM?
No
Yes
Next CVM in CVM List processing EMV4.3iii 10.5
Enciphered PIN?
Yes
No
Issue GET CHALLENGE EMV4.3iii 6.5.6 and EMV4.3ii 7.1 & 7.2
TVR: Cardholder Verification was not successful CVM Results set as EMV4.3iv 6.3.4.5
PIN returned from PIN Pad
Issue VERIFY EMV4.3iii 6.5.12
CVM Results: 'Successful' CVM Processing Complete
Yes
PIN OK? SW=9000
No
PIN Tries left in SW
10 Terminal Risk Management

Figure 9-3: Offline PIN Terminal Process Flow

All AEIPS-compliant Chip Cards supporting offline PIN verification also support the GET DATA command as defined in [EMV4.3iii] Section 6.5.7, for the retrieval of the *Remaining PIN Try Counter*.

Following *Cardholder Verification Method (CVM) List* processing if the chosen CVM for the transaction is Offline PIN or Offline Enciphered PIN, the Terminal ***must*** issue the GET DATA Command to retrieve the *Remaining PIN Try Counter* from the Chip Card.

- If the value of the *Remaining PIN Try Counter* is zero the Terminal ***must*** perform the following:
  - Set the 'PIN Try Limit Exceeded' bit to "1" in the TVR
  - Perform the action specified by the *Cardholder Verification Method (CVM) List* entry (i.e., Fail Cardholder Verification, or apply next CVM) and proceed to Terminal Risk Management, Section 10, or CVM List Processing in Figure 9-2.
- Else If the value of the *Remaining PIN Try Counter* is "1" the Terminal should display a message to indicate that there is only one PIN Try Remaining, such as 'Last PIN Try'.

- Else If the value of the *Remaining PIN Try Counter* is greater than zero the Terminal should prompt for PIN Entry.
- If the CVM for the transaction is offline enciphered PIN then prior to issuing a VERIFY Command the Terminal ***must*** issue a GET CHALLENGE Command to the Chip Card, as defined in [EMV4.3iii] Section 6.5.6. The Terminal ***must*** proceed with enciphered PIN key selection as described in [EMV4.3ii] Section 7.1 and processing as defined in [EMV4.3ii] Section 7.2.
- Following the entry of the Offline PIN the Terminal ***must*** issue the VERIFY Command to the Card including the Transaction PIN Data, as defined in [EMV4.3iii] Section 6.5.12. PIN verification will then be performed by the Chip Card.

There are four possible outcomes of the PIN Verification performed by the Chip Card that the Terminal ***must*** handle:

1 PIN Verified OK - If the PIN is successfully verified by the Chip Card, the Card will return SW1 SW2 equal to '9000' and the Terminal ***must*** confirm correct PIN entry to the Cardholder displaying a 'PIN OK' message or similar. Cardholder CVM is successful and processing continues with Terminal Risk Management.

2 PIN Incorrect and PIN Try Limit Not Exceeded - If the PIN verification by the Chip Card is not successful and SW1 SW2 equal to '63Cx' is returned by the Chip Card (where 'x' is the number of PIN tries remaining), the Terminal should display a message 'INCORRECT PIN' and additionally a message indicating the number of attempts remaining (e.g., '2 PIN TRIES REMAINING' if x = 2). If the Chip Card returns SW1 SW2 equal to '63C1' indicating one PIN try remaining, the Terminal may display a message 'LAST PIN TRY' or similar.

3. PIN Incorrect and *PIN Try Limit* Exceeded on this transaction - If the PIN verification by the Chip Card is not successful and SW1 SW2 equal to "63C0" is returned by the Chip Card indicating zero remaining PIN try attempts, the Terminal ***must*** perform the following:

   - Set the TVR byte 3 bit 6 ("PIN Try Limit Exceeded") to "1".
   - Perform the action specified by the *Cardholder Verification Method (CVM) List* entry (i.e., Fail Cardholder Verification, or apply next CVM) and proceed to Terminal Risk Management, Section 10 or CVM List Processing in Figure 9-2.

4. *PIN Try Limit* Exceeded on Previous Transaction - If the PIN verification by the Chip Card is not successful and SW1 SW2 equal to '6983' or '6984' is returned by the Chip Card indicating that the *PIN Try Limit* exceeded on a previous transaction, the Terminal ***must*** perform the following:

   - Set the TVR byte 3 bit 6 ("Offline PIN Try Limit Exceeded") to "1".
   - Perform the action specified by the *Cardholder Verification Method (CVM) List* entry (i.e., Fail Cardholder Verification, or apply next CVM) and proceed to Terminal Risk Management Section 10 or CVM List Processing in Figure 9-2.

9.3.3 Other CVM

Other CVMs (e.g. signature, No CVM, combination CVM) are processed as per [EMV4.3iii] Section 10.5.

9.4 PIN Pad Requirements

If a PIN Pad is present, it ***must*** comply with EMV requirements as defined in [EMV4.3ii] Section 11.1, the PCI Security Standards Council PIN Transaction Security (PTS) requirements and guidelines and any additional local market requirements. American Express has no minimum requirements for PIN Pads above those of EMV, the PCI and the local market payment authorities or regulatory bodies.

10 Terminal Risk Management

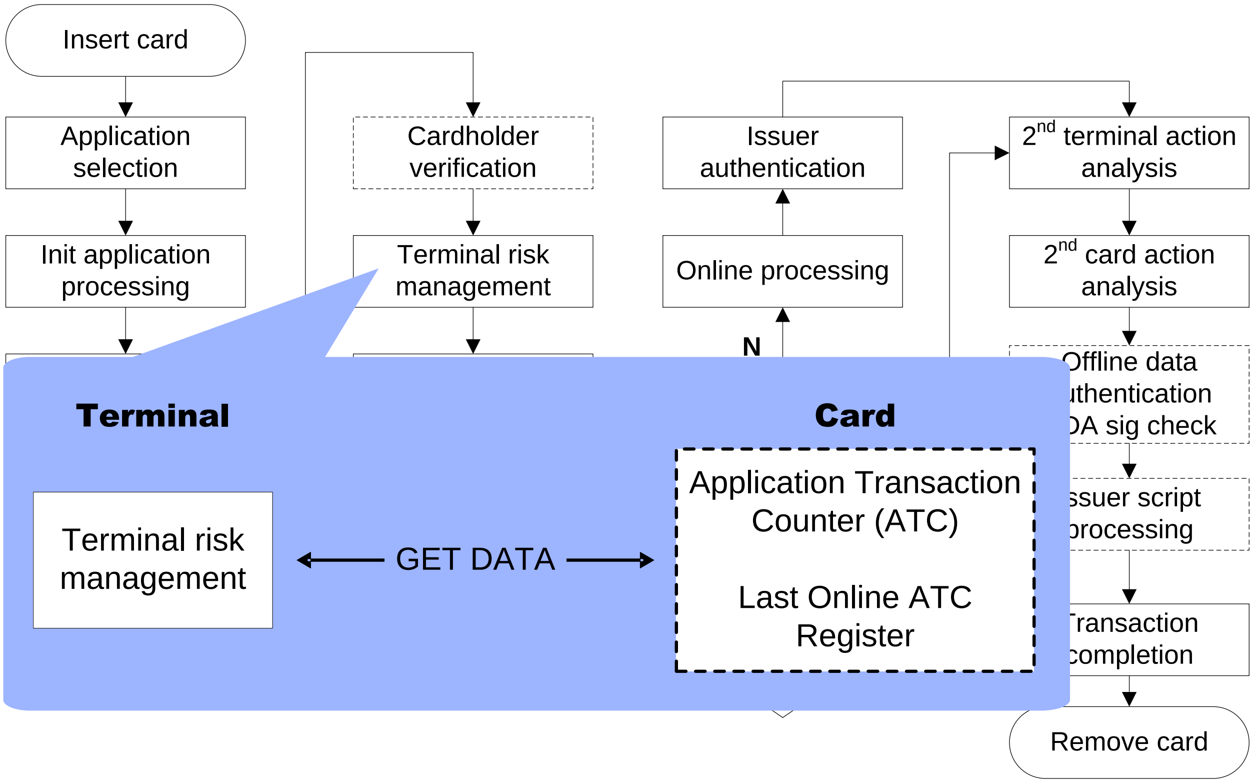

Figure 10-1: Terminal Risk Management Detail

10.1 Overview

Terminal Risk Management performs a series of checks to determine whether:

- The transaction is over the merchant Network Floor Limit
- The account number is on an ***optional*** Terminal exception file
- The Terminal limit for consecutive offline transactions has been exceeded
- The Chip Card is a new Chip Card
- The Merchant has forced the transaction online.

Some transactions are randomly selected for online processing. The results of the risk management check are stored in a Terminal resident data element called *Terminal Verification Results (TVR)*. All the required EMV-defined risk management checks are performed by the Terminal. Terminal processing decisions based on the outcome of the above checks are configurable, as determined by the Chip Card (for the Issuer) and Terminal resident data elements (for the Merchant and Acquirer) which are the *Issuer Action Codes* and the *Terminal Action Codes* respectively (See Section 11).

10.2 Commands

- GET DATA

To support the EMV Terminal Risk Management processes, the Terminal will support the GET DATA command as defined in [EMV4.3iii] Section 6.5.7 GET DATA Command-Response APDUs.

10.3 Processing Requirements

Terminal Risk Management ***must*** always be performed as stated in [EMV4.3iii] Section 10.6 and [EMV4.3iv] Section 6.3.5. Random transaction selection need not be performed by a Terminal without online capability.

Online-capable Terminals and merchants ***must*** support random transaction selection and ***optionally*** a Terminal Exception File. If the transaction is randomly selected for online authorization then the TVR byte 4, bit 5 ***must*** be set to “1”. If the Terminal Exception File is used and a match is found then the TVR byte 1, bit 5 ***must*** be set to “1”.

The results of the risk management check ***must*** be stored in the TVR (as defined in Section 22.3.7).

Terminals ***must*** use the GET DATA Command as defined in [EMV4.3iii] Section 6.5.7 to retrieve the *ATC* (tag ‘9F36’) and the *Last Online Application Transaction Counter register* (tag ‘9F13’). This is used in Terminal Velocity Checking, as defined in [EMV4.3iii] Section 10.6.3. If the data is missing or erroneous the TVR byte 1, bit 6 (Card data missing) ***must*** be set to “1” according to [EMV4.3iii] Section 7.5 Table 31. If the *Last Online Application Transaction Counter register* value is zero then the Terminal ***must*** set the TVR byte 2, bit 4 (New Card) to “1” as per [EMV4.3iii] Section 10.6.3.

Terminals may allow a merchant to force a transaction online, for example if the merchant is suspicious. If this occurs the Terminal must set the TVR byte 4, bit 4 (Merchant forced transaction online) to “1” as per [EMV4.3iv] Section 6.5.3.

Where possible, terminals should be configured with a Chip Transaction Floor Limit that is distinct from the non-Chip Transaction Floor Limit. This feature allows Chip Card transactions to have their risk managed separately from magnetic stripe or manual entry transactions.

11 1st Terminal Action Analysis

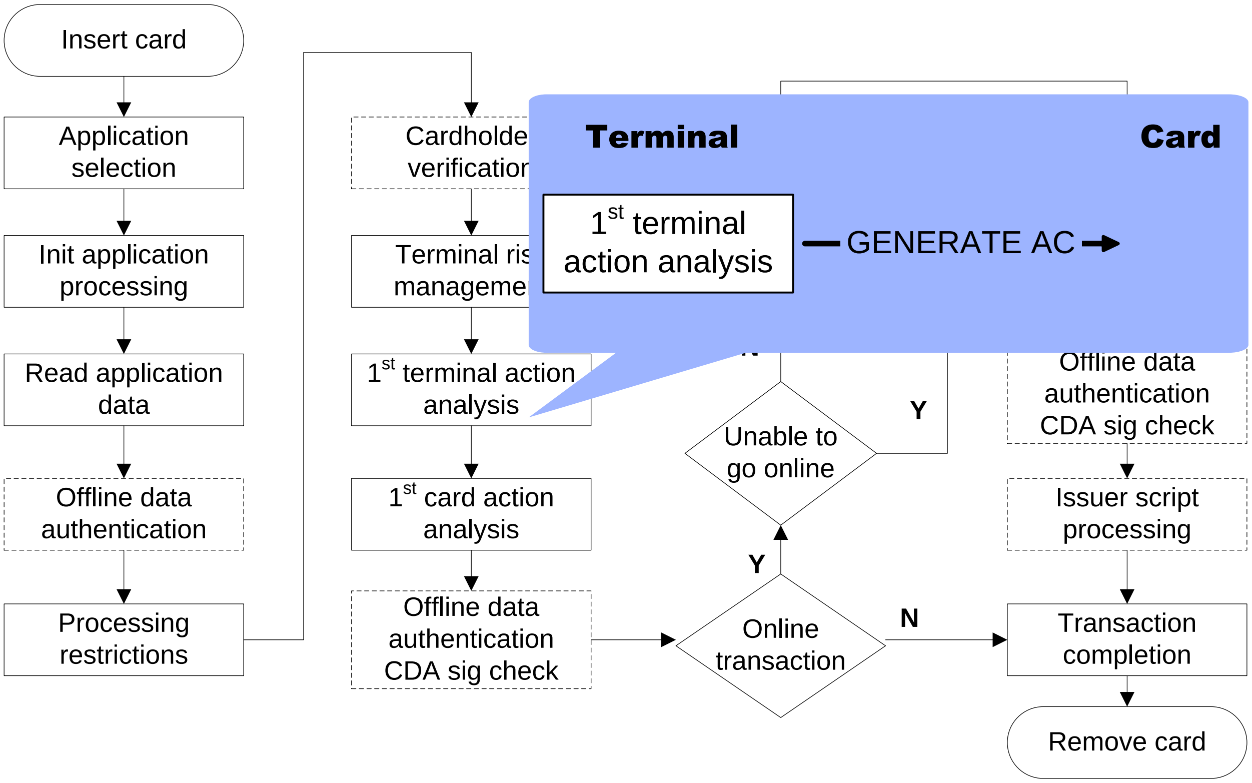

Figure 11-1: Terminal Action Analysis Detail

11.1 Overview

1st Terminal Action Analysis uses the results of Offline Data Authentication, Processing Restrictions, Terminal Risk Management, Cardholder Verification (collectively known as offline-processing results) and rules set in the Chip Card and Terminal to determine whether the transaction should be approved offline, sent online for authorization, or declined offline.

The Chip Card rules are set by the Issuer in fields called *Issuer Action Codes (IACs)* sent to the Terminal by the Chip Card. American Express rules are set in *Terminal Action Codes (TACs)* configured into the Terminal. After determining the transaction disposition, the Terminal requests an *Application Cryptogram* from the Chip Card. The Terminal processes the results with the rules to determine the type of *Application Cryptogram* to request from the Chip Card.

11.2 Processing Requirements

The type of *Application Cryptogram* requested ***must*** be based upon the transaction disposition with a *Transaction Certificate (*TC*)* for an approval, an *Authorization Request Cryptogram (*ARQC*)* for a request to go online, and an *Application Authentication Cryptogram (*AAC*)* for a decline as defined in [EMV4.3iii] Section 10.7 and [EMV4.3iv] Section 6.3.6.

Note that [EMV4.3iii] Section 10.7 states "The Terminal action analysis function may be executed at several places during a transaction to eliminate the need for unnecessary processing". In line with [EMV4.3iii] AEIPS also maintains this flexibility.

1st Terminal Action Analysis comprises two stages:

- Checking of the Offline Processing Results
- Requesting a Cryptogram from the Card.

11.2.1 Offline Processing Results

The Terminal ***must*** examine the results of Offline processing recorded in the *TVR* during the Transaction so far, for example, during Terminal Risk Management.

The review of the offline processing results ***must*** be performed against the *Issuer Action Codes (IACs)* read from the Chip Card during the 'Read Application Data' phase of the transaction, and the *Terminal Action Codes (TACs)* resident in the Terminal.

The Terminal compares bit settings in the *Issuer Action Codes* and *Terminal Action Codes* to the corresponding bits in the TVR*.* Setting of the corresponding bit in either the *IACs* or *TACs* will determine the outcome of the Terminal action analysis as described further below.

There are three sets of *Issuer Action Codes* and corresponding *Terminal Action Codes*:

Table 11-1: Issuer Action Codes and corresponding Terminal Action Codes

Issuer Action Code - Denial Terminal Action Code - Denial	Defines conditions that determine if the Terminal **must** request that the transaction be declined offline
Issuer Action Code - Online Terminal Action Code - Online	Defines conditions that determine if the Terminal **must** request that the transaction be transmitted online for authorization
Issuer Action Code – Default Terminal Action Code - Default	Defines conditions that determine if the Terminal **must** request a transaction be declined that was required to be sent online but that the Terminal is unable to send online

The processing to be performed by the Terminal ***must*** be as follows:

The Terminal ***must*** compare the *Issuer Action Codes - Denial* and *Terminal Action Codes - Denial* with the results of the current transaction as recorded in the TVR, and if any of the corresponding bits are set, the transaction is requested to be declined and the Terminal ***must***:

- Set the Cryptogram type to be requested in the GENERATE AC Command to *Application Authentication Cryptogram (AAC).*
- Set the *Authorization Response Code*[1] *(ARC)* to value "Z1" indicating 'Offline Decline'.
- Proceed to Section 11.2.2.

If the Action Codes and TVR do not indicate that an AAC is required, the subsequent processing is determined by the capability of the Terminal to go online:

1. If the Terminal has the capability to connect online for authorization, the Terminal ***must*** compare the *Issuer Action Codes - Online* and *Terminal Action Codes - Online* with the results of the current transaction as recorded in the TVR*,* and if any of the corresponding bits are set, the Transaction is requested to be transmitted online for authorization and the Terminal ***must***:
   - Set the Cryptogram type to be requested in the GENERATE AC Command to Authorization Request Cryptogram (ARQC).
   - Proceed to Section 11.2.2.
2. If the Terminal has the capability to connect online for authorization, but none of the corresponding bits in the Decline and Online Action Codes are set, the transaction is requested to be approved offline and the Terminal ***must***:
   - Set the Cryptogram type to be requested in the GENERATE AC Command to Transaction Certificate Cryptogram (TC).
   - Set the *Authorization Response Code (ARC)* to value "Y1" indicating 'Offline Approved'.

[1] While the Authorization Response Code is not submitted to the Chip Card with the 1st GENERATE AC it is important that the Terminal still set it during 1stTerminal Action Analysis for settlement, advice and receipt printing purposes.

  - Proceed to Section 11.2.2.

3. If the Terminal does not have the capability to connect online, or the online transaction cannot complete, the Terminal ***must*** compare the *Issuer Action Codes - Default* and *Terminal Action Codes - Default* with the results of the current transaction as recorded in the TVR*,* and if any of the corresponding bits are set, the transaction is requested to be declined and the Terminal ***must***:
   - Set the Cryptogram type to be requested in the GENERATE AC Command to Application Authentication Cryptogram (AAC).
   - Set the *Authorization Response Code (ARC)* to value “Z3” indicating ‘Offline Decline as Unable to go Online’.
   - Proceed to Section 11.2.2.
4. If the terminal has requested and obtained an online PIN from the cardholder for verification, the terminal ***must not*** request an offline approval from the Chip Card regardless of other risk settings (including *IACs* or *TACs*).
5. If none of the above checks result in the Transaction being declined or sent online for authorization, the transaction is requested to be approved offline and the Terminal ***must***:
   - Set the Cryptogram type to be requested in the GENERATE AC Command to Transaction Certificate Cryptogram (TC).
   - Set the *Authorization Response Code (ARC)* to value “Y3” indicating ‘Offline Approved as Unable to go Online’.
   - Proceed to Section 11.2.2.

11.2.2 Request Application Cryptogram in 1st GENERATE AC

The 1st Terminal Action Analysis processing concludes with the issuance of the 1st GENERATE AC Command to the Chip Card, as defined in [EMV4.3iii] Section 6.5.5. The Terminal ***must*** format the GENERATE AC Command to request a TC, an AAC, or an ARQC from the Chip Card dependent on the results of the review of the offline processing results described in Section 11.2.1.

- A request for a TC indicates that the Terminal is requesting that the Transaction be approved offline.
- A request for an AAC indicates that the Terminal is requesting that the transaction be declined offline.
- A request for an ARQC indicates that the Terminal is requesting that the transaction be sent online for authorization.

As a result of the issuance of the GENERATE AC Command by the Terminal the Chip Card will (on completion of any Card Risk Management) return an Application Cryptogram to the Terminal. The Card may in some circumstances override the Terminal’s decision for the Transaction disposition (Approve, Decline, Go Online) in accordance with the rules defined in 1st Card Action Analysis (See Section 12).

An *Application Cryptogram* ***must*** be requested using the GENERATE AC command, as defined in [EMV4.3iii] Section 6.5.5 GENERATE APPLICATION CRYPTOGRAM Command-Response APDUs.

If the Chip Card supports CDA and the Terminal is to request an ARQC, then the Terminal ***must*** determine if CDA is to be requested in the 1st GENERATE AC through a configured *CDA Mode*, as described in [EMV4.3ii] Annex D4.

When CDA is required the terminal ***must*** set the “CDA signature requested” bit in the Reference Control Parameter of the GENERATE AC command and the Terminal ***must*** perform CDA upon receipt of the GENERATE AC response as defined in [EMV4.3ii] Section 6.6.

12 1st Card Action Analysis

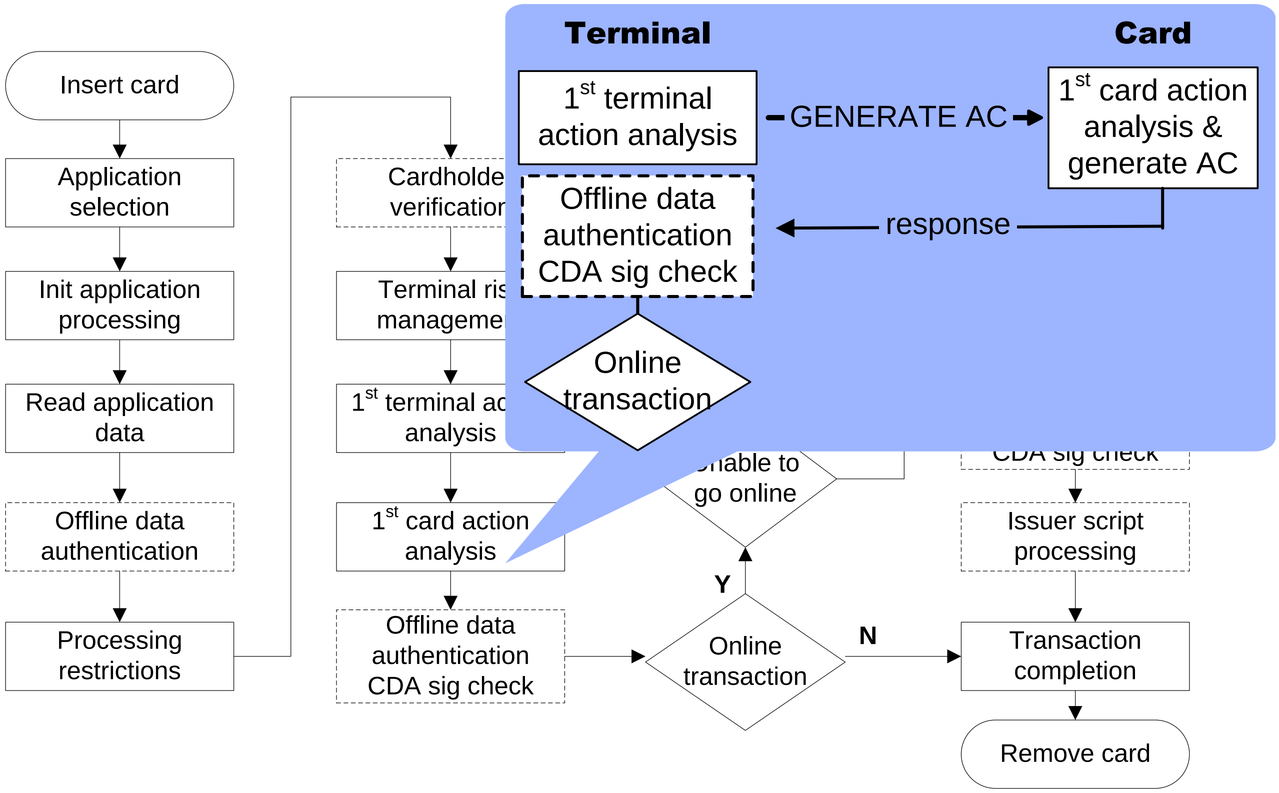

Figure 12-1: 1st Card Action Analysis Detail

12.1 Overview

Upon receiving the 1st GENEATE AC command from the Terminal, the Chip Card performs the 1st Card Action Analysis where Card Risk Management checks are performed to determine the response to the request for a cryptogram. The Chip Card may convert a Terminal request for an offline approval to an online transaction or an offline decline. Similarly, the Chip Card may convert a Terminal request for an online transaction to an offline decline.

After completion of the checks, the Chip Card generates the *Application Cryptogram* using application data and a secret key stored on the Chip Card. It returns this cryptogram to the Terminal.

For offline-approved transactions, a TC cryptogram is generated. The TC provides non-repudiation evidence of the transaction. When a TC is generated the Terminal does not request a second cryptogram from the Chip Card and the Terminal moves directly to the processing defined in Transaction Completion (See Section 18).

For offline-declined transactions, the cryptogram generated by the card is an AAC. The AAC and the data used to generate it may be transmitted in an advice message where such messages are supported. Furthermore, a specially designated Terminal may still request online authorization using the AAC in the message to the Issuer if the terminal application is to support the delivery of Issuer Scripts to the Chip Card e.g. to perform functions such as unblocking the application.

For transactions to be authorized online, the Chip Card responds with an ARQC cryptogram. In this case the Terminal moves directly to the processing described in Online Processing (See Section 13), unless the Terminal does not have online capability, in which case it proceeds straight to 2nd Terminal Action Analysis (See Section 15).

The *Application Cryptogram* (AC) produced by the Chip Card in response to a GENERATE AC command, is used by the Issuer of the Chip Card to validate the transaction and the Chip Card.

If the Terminal requests CDA then the process “Offline Data Authentication CDA sig check” is performed and the card generates a dynamic signature that is returned to the terminal with the Application Cryptogram. The terminal validates the returned signature.

12.2 Commands

- GENERATE AC

The processing described in this section is triggered when the Terminal sends a GENERATE AC command for the first time within a single financial transaction.

The response to the GENERATE AC command uses Format 1 as defined in [EMV4.3iii] Section 6.5.5.4.

12.3 Processing Requirements

1st Card Action Analysis processing in the Chip Card is triggered by the Terminal issuing the Chip Card a GENERATE AC command. The Terminal is informed of the result of this process in the response data returned by the Chip Card.

If the Terminal requested a TC from the Card, then the permitted responses from the Card include a TC, ARQC or AAC and processing continues.

If the Terminal requested an ARQC from the Card, then the permitted responses from the Card include either an ARQC or AAC and processing continues. Otherwise processing ***must*** terminate.

If the Terminal requested an AAC from the Card, then the permitted response from the Card includes an AAC and processing continues. Otherwise processing ***must*** terminate.

Valid responses which include a TC or AAC signal that the transaction is to be completed offline and processing can move to Section 18 following a CDA check, if required.

A valid response containing an ARQC signals that an online authorization is required and processing moves to Section 13 following a CDA check, if required.

When CDA is being performed the Card will create a dynamic signature that includes the TC or ARQC. The Terminal ***must*** use the CAPK to validate the dynamic signature as described in [EMV4.3ii] Section 6.6. If an AAC is returned then CDA is not performed by the terminal as per [EMV4.3ii] Section 6.6.

If CDA fails, the Terminal ***must*** perform the processing defined in [EMV4.3iv] Section 6.3.2, in particular:

- The Terminal ***must*** set TVR byte 1 bit 3, indicating that CDA failed
- If the Cryptogram Information Data (CID) indicates a TC was returned by the card, the Terminal ***must*** decline the transaction without issuing a 2nd GENERATE AC command
- If the CID indicates that an ARQC was returned by the card, the Terminal ***must*** immediately issue a 2nd GENERATE AC command, requesting an AAC (transaction decline).

13 Online Processing

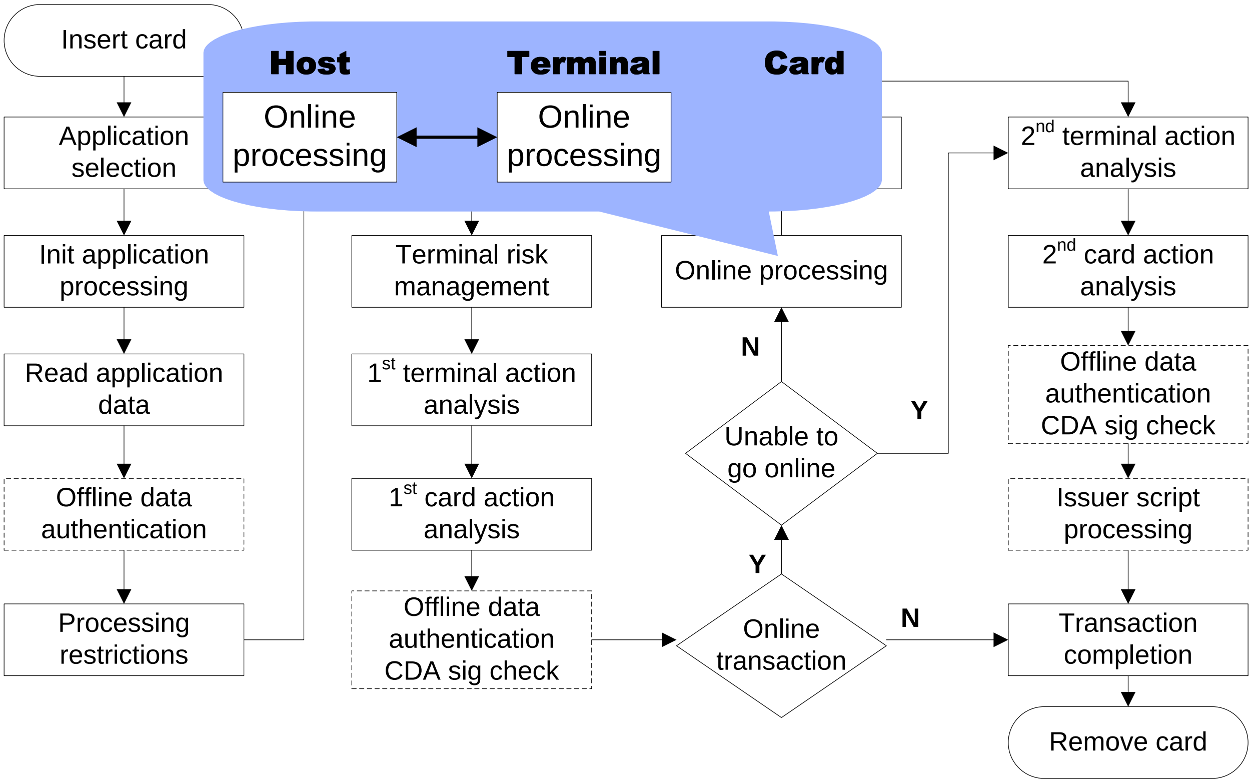

Figure 13-1: Online Processing Detail

13.1 Overview

If the Chip Card or Terminal determines that the transaction requires an online authorization and the Terminal has online capability, then the Terminal transmits an online authorization message to the Issuer. This message includes the cryptogram generated by the Chip Card, the data used to generate the cryptogram and indicators showing offline processing results.

An online authorization request is initiated when the response to the 1st GENERATE AC command is an *ARQC*.

The authorization response message transmitted back to the Terminal may include an Issuer-generated *Authorization Response Cryptogram (ARPC)*. The response may also include post-issuance updates to the Chip Card called Issuer Scripts.

13.2 Processing Requirements

Online Processing ***must*** follow the procedures defined in [EMV4.3iii] Section 10.9 and [EMV4.3iv] Section 6.3.8. Online processing facilitates card authentication and authorization in the Issuer's host computer and to reach a decision on how to respond to the authorization request using the Issuer's host-based risk management parameters.

One of four Terminal actions can follow an Online Authorization Request (ARQC) being generated.

- **The Terminal connects to the Acquirer and Issuer Authentication Data (tag '91') is returned.** On receipt of the Chip Card data the Terminal ***must*** pass the *Issuer Authentication Data* received from the Acquirer to the Chip Card in the EXTERNAL AUTHENTICATE command as part of Issuer Authentication (See Section 14).
- **The Terminal connects to the Acquirer but no Chip Card response data is returned from the Acquirer.** On receipt of the Chip Card data a magnetic stripe or 'downgraded' response indicator is

received, the Terminal ***must*** derive the *Authorization Response Code* based on the data received from the Acquirer. The *Authorization Response Code* is passed to the Chip Card in the 2nd GENERATE AC Command. In this case, the Terminal ***must*** proceed to 2nd Terminal Action Analysis (See Section 15) without performing Issuer Authentication.

- **The Terminal is unable to connect to the Acquirer for online authorization (offline device or communications failure).** The Terminal ***must*** proceed to 2nd Terminal Action Analysis as detailed in Section 15 without performing Issuer Authentication. The decision process for acceptance or rejection of the transaction ***must*** be determined by checking the "Default" *Issuer Action Codes* in use for that Chip Card application.
- **The Terminal is connected to the Acquirer/Issuer and the Issuer responded with a 'voice referral response'.** In many cases a voice referral will require the card to be taken to a separate location in order for the referral to be completed (i.e., a phone point) as information on the back of a card may be asked for during the referral process. In order for the card to be left in a clean state, the transaction should continue and the Terminal should request either a TC or an AAC so that the card can be withdrawn. The terminal should display a 'call card Issuer' or similar prompt.

14 Issuer Authentication

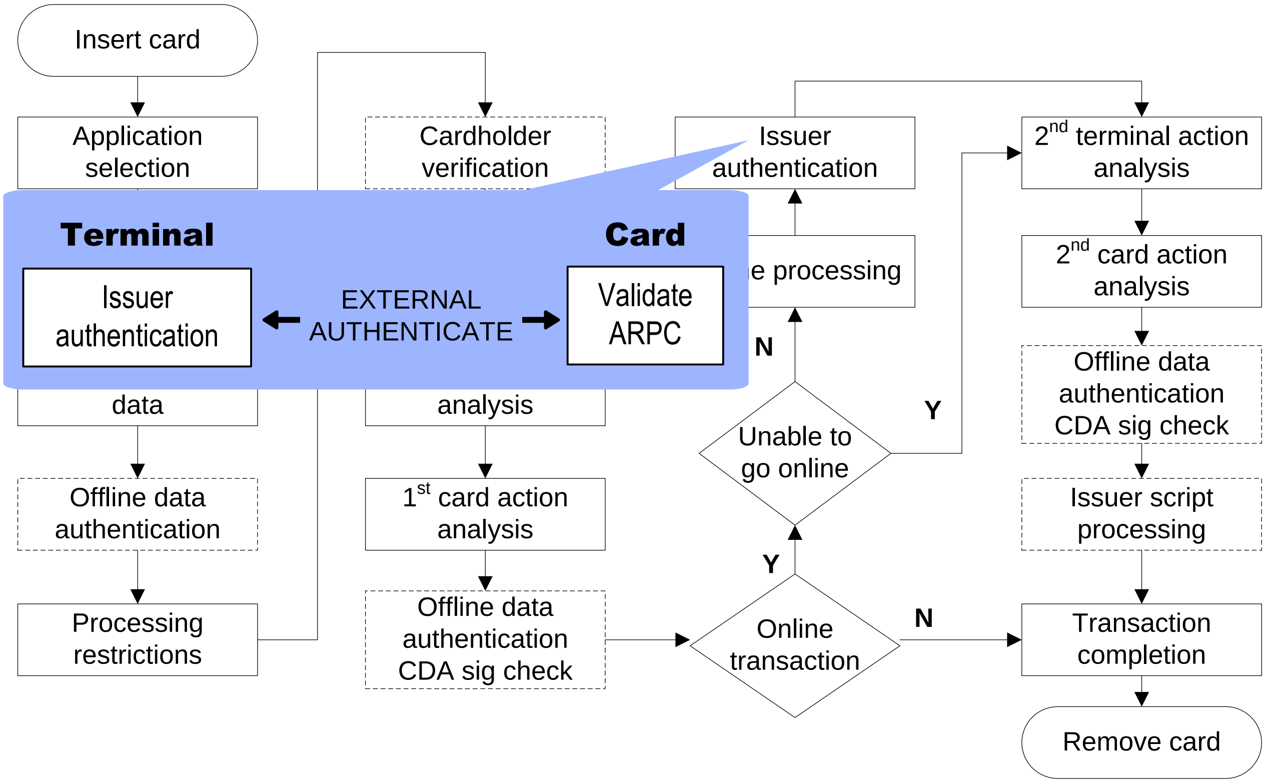

Figure 14-1: Issuer Authentication Detail

14.1 Overview

Optionally, the Issuer may return *Issuer Authentication Data* in the response to the online request from the Terminal. The Terminal sends this data to the Chip Card which uses it to authenticate that the Issuer host and response data is genuine.

If Online Processing does not conclude with the Terminal receiving *Issuer Authentication Data*, the Terminal continues to 2nd Terminal Action Analysis (See Section 15).

The response from the Issuer may also include post-issuance updates to the Chip Card known as Issuer Scripts (See Section 17).

14.2 Commands

- EXTERNAL AUTHENTICATE

This command is used in performing Issuer Authentication. The Terminal transmits to the Chip Card a data object called the *Issuer Authentication Data,* as defined in [EMV4.3iii] Section 6.5.4. This data ***must*** contain the ***mandatory*** *Authorization Response Cryptogram (ARPC)* and *Authorization Response Code*. The *Issuer Authentication Data* ***must*** consist of the following data:

- ARPC (eight bytes)
- Authorization Response Code (two bytes).

14.3 Processing Requirements

If Online Processing concludes with the Terminal receiving *Issuer Authentication Data*, the Terminal ***must*** perform Issuer Authentication.

Issuer Authentication is performed by the Terminal passing *Issuer Authentication Data*, received in the Chip Card authorization response message from the Issuer, to the Chip Card in an EXTERNAL AUTHENTICATE command.

EXTERNAL AUTHENTICATE ***must*** be performed as described in [EMV4.3iii] Section 6.5.4. If Issuer Authentication fails the TVR byte 5 bit 7 (Issuer authentication was unsuccessful) is set to “1” as per [EMV4.3iii] Annex F.

15 2nd Terminal Action Analysis

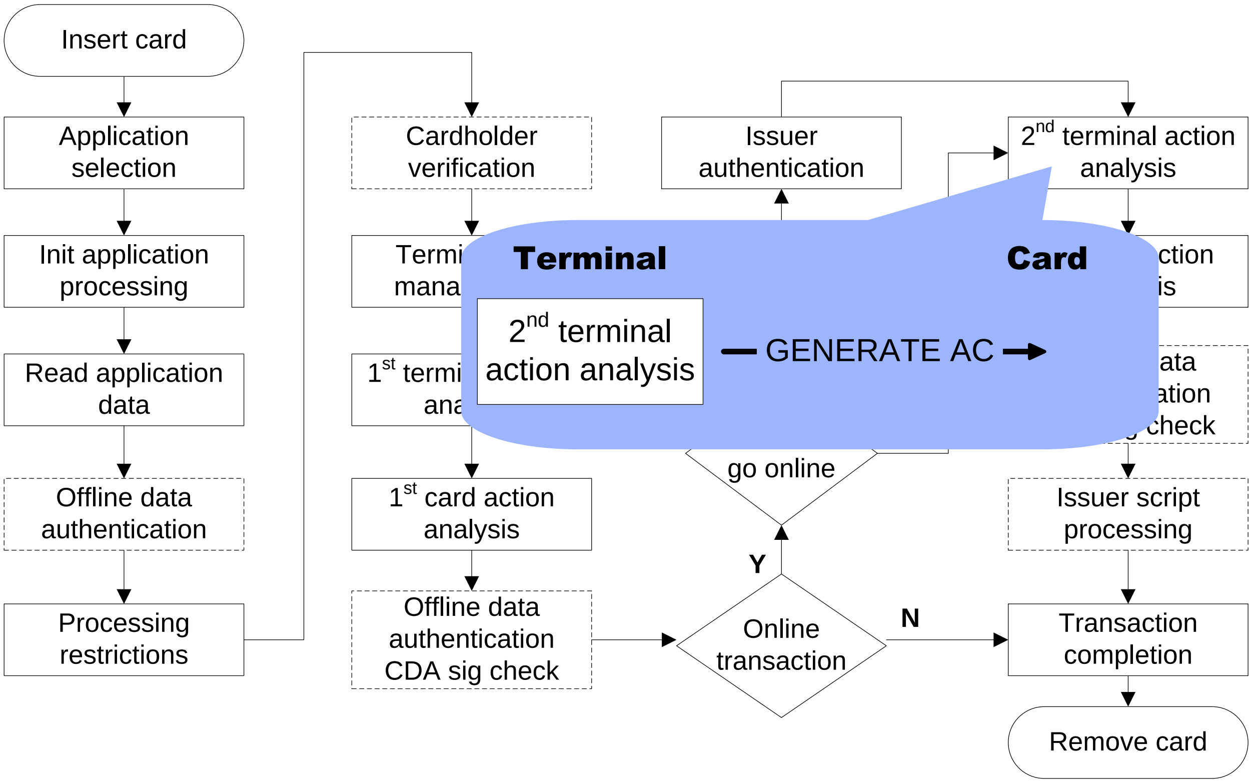

Figure 15-1: 2nd Terminal Action Analysis Detail

15.1 Overview

Once any online processing is complete, the Terminal decides how to complete the transaction. In 2nd Terminal Action Analysis there are three distinct cases:

- **Online (Card Authenticated by Issuer):** The Issuer has successfully processed the transaction and provided a response to the Terminal containing *Issuer Authentication Data*.
- **Online (Card not Authenticated by Issuer):** The Issuer has processed the transaction and provided a response to the Terminal without any *Issuer Authentication Data* in the Response.
- **Unable to go Online:** The Terminal was unable to go online or the connection to the Issuer failed before a complete Response was received.

The Terminal processes the results and requests approval or decline from the Chip Card.

2nd Terminal Action Analysis occurs only if an ARQC was produced by the card in response to the 1st GENERATE AC command.

15.2 Processing Requirements

The Terminal ***must*** check the results from Online Processing to determine which cryptogram type (AAC or TC) to request the card to generate.

If the Terminal went online and *Issuer Authentication Data* (tag ‘91’) was returned by the Issuer, the Terminal ***must*** request a 2nd Generate Application Cryptogram and the *Authorization Response Code* submitted in the command data for the 2nd GENERATE AC command ***must*** be the value provided as part of the *Issuer Authentication Data*.

If the Terminal went online and receives an authorization response that does contain valid information regarding the transaction result, but does not contain the required chip data to perform Issuer Authentication

(*Issuer Authentication Data*), this is known as a downgraded transaction. In this case the terminal derives the *Authorization Response Code* based on local requirements for the disposition of the response message returned by the Acquirer. The Terminal ***must*** populate the *Authorization Response Code* (EMV tag ‘8A’) to be returned to the Chip Card in the 2nd GENERATE AC command as follows:

- “00” for an approval result coded in ASCII (i.e. hexadecimal “3030”).
- “02” for a referral result coded in ASCII (i.e. hexadecimal “3032”).
- “05” for a decline coded in ASCII (i.e. hexadecimal “3035”).

If the Terminal was unable to go online it ***must*** send an *Authorization Response Code* (Tag ‘8A’) set to “Z3” (unable to go online, offline declined) or “Y3” (unable to go online, offline approved) to the Card as part of the command data in the 2nd GENERATE AC command. The Terminal ***must*** determine whether to request offline approval or offline decline from the Chip Card dependent upon the *Terminal Action Codes* resident in the Terminal and the *Issuer Action Codes* read from the Chip Card.

An *Application Cryptogram* ***must*** be requested using the GENERATE AC command, as defined in [EMV4.3iii] Section 6.5.5.

If the Chip Card supports CDA and the Terminal is to request a TC, then the Terminal ***must*** determine if CDA is to be requested in the 2nd GENERATE AC through a configured *CDA Mode*, as described in [EMV4.3ii] Annex D4.

When CDA is required the terminal ***must*** set the “CDA signature requested” bit in the Reference Control Parameter of the GENERATE AC command and the Terminal ***must*** perform CDA upon receipt of the GENERATE AC response as defined in [EMV4.3ii] Section 6.6.

15.2.1 Advice Messages

When the Terminal receives a response to a GENERATE AC command, it includes the *CID*, a data element that indicates if the card has requested an advice message be created. Cards may set bits requesting advice depending on card personalization for a particular AEIPS-compliant payment application.

If the Card has indicated that an advice is required in the *CID,* the Terminal decides what action to take, if any. For instance, if the Terminal is required to transmit a data capture record or a reversal message for that transaction; it is not necessary for the Terminal to also transmit an advice. If the Terminal is required to transmit an advice, the Terminal ***must*** determine whether to transmit an offline or online advice based upon its capabilities and any local market requirements. American Express does not require advices to be supported unless stipulated by local market conditions.

15.2.2 Voice Referrals

If a voice referral has been received the Terminal ***must*** complete the transaction by issuing a 2nd GENERATE AC command for either an AAC or a TC before the card is removed and the referral is made (section 18.2.1).

16 2nd Card Action Analysis

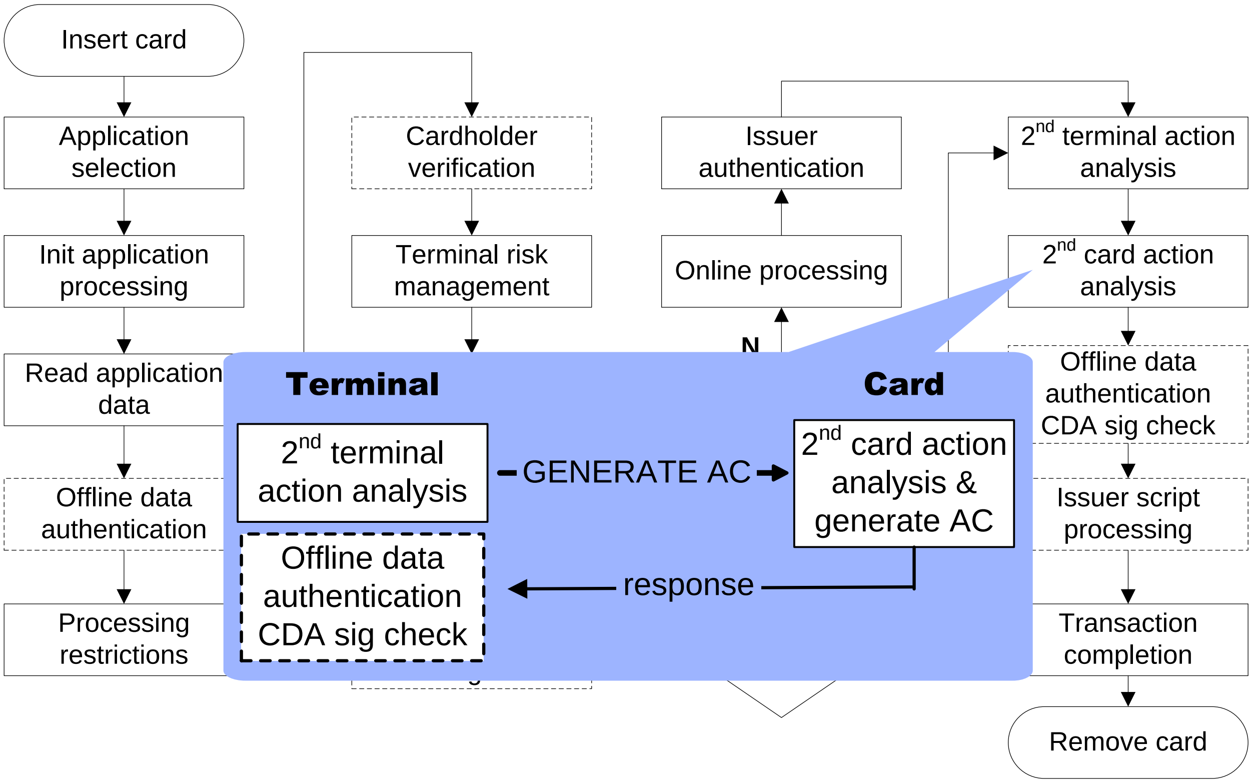

Figure 16-1: 2nd Card Action Analysis Detail

16.1 Overview

This function is only performed if the Terminal asks the Chip Card to generate a 2nd Application Cryptogram. The Chip Card may decline an Issuer-approved transaction based upon the Issuer Authentication results and Issuer-encoded parameters in the Chip Card.

The Chip Card generates a TC for approved transactions and an AAC for declined transactions.

The Chip Card may set or reset certain security-related parameters in the Card at this point.

16.2 Commands

2nd Terminal Action Analysis processing concludes with the Terminal issuing a 2nd GENERATE AC command to the Chip Card. The *AC* returned in response to the GENERATE AC.

Issuer Application Data will be included in the data returned by the Chip Card in response to a GENERATE AC command. The *Issuer Application Data* is a ***mandatory*** data object in this manual used to transmit proprietary data from the Chip Card to the Terminal for input to the online request message or clearing record.

The GENERATE AC command ***must*** either indicate that the Terminal requests that the Chip Card approves (TC requested) or declines (AAC requested) the transaction.

The 2nd GENERATE AC command may only be performed in the following cases:

- After an ARQC has been returned to the 1st GENERATE AC command
- When the application is blocked and an AAC has been returned to the 1st GENERATE AC command.

16.3 Processing Requirements

The Terminal is not involved in the 2nd Card Action Analysis, however it is triggered by the Terminal issuing the Chip Card a GENERATE AC command requesting either a TC or AAC, depending on the results of 2nd Terminal Action Analysis.

The Terminal ***must*** send a 2nd GENERATE AC Command to the Chip Card, requesting either the transaction be declined (AAC) or approved (TC) according to the result of 2nd Terminal Action Analysis

The Terminal is informed of the result of this process in the response data returned by the Chip Card.

If the Terminal requested a TC from the Card, then the permitted responses from the Card include either a TC or AAC and processing continues. Otherwise processing ***must*** terminate.

If the Terminal requested an AAC from the Card, then the permitted responses from the Card include an AAC and processing continues. Otherwise processing ***must*** terminate.

At this point the transaction is ready to be completed following a CDA check, if required and any Script Processing in Section 17. When CDA is being performed the Card will create a dynamic signature that includes the TC. The Terminal ***must*** use the CAPK to validate the dynamic signature as described in [EMV4.3ii] Section 6.6. If an AAC is returned then CDA is not performed by the terminal as per [EMV4.3ii] Section 6.6.3 Figure 5.

If CDA fails, the Terminal ***must*** perform the processing defined in [EMV4.3iv] Section 6.6.2, in particular:

- The Terminal ***must*** set TVR byte 1 bit 3, indicating that CDA failed
- If the Cryptogram Information Data (CID) indicates a TC was returned by the card, the Terminal ***must*** decline the transaction.

17 Issuer Script Processing

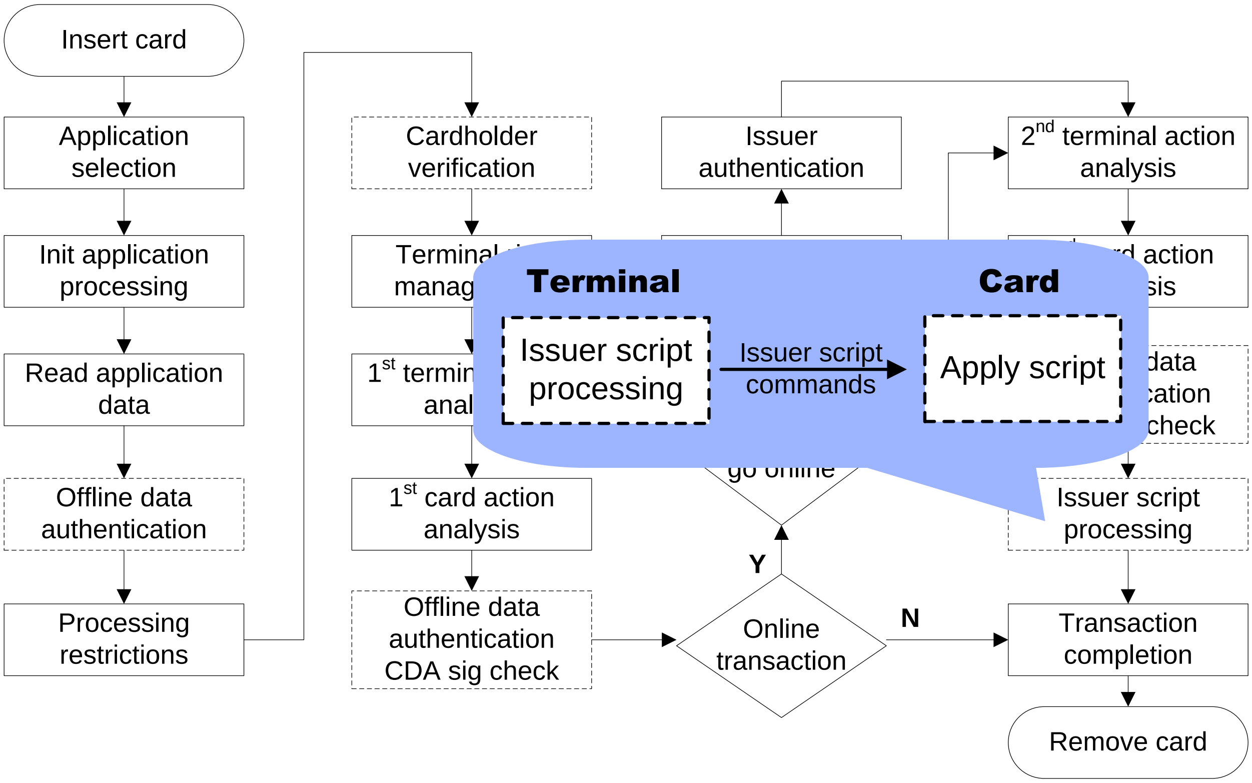

Figure 17-1: Issuer Script Processing Detail

17.1 Overview

If the Issuer included script updates in the authorization response message returned in "Online Processing", the Terminal passes the script commands to the Chip Card after it has returned the final *Application Cryptogram*.

Issuer Script Processing is performed to allow the Issuer to adjust or update data on the Chip Card. The functions supported by Issuer Script Processing in an AEIPS card are:

- Maintenance of Risk Management Parameters
- Control of Chip Card Use
- Maintenance of Personal Identification Number (PIN).

EMV allows Issuer Script Processing in other places during the transaction. However, for this version of AEIPS, a Card only processes Issuer Scripts received at this point in the transaction. That is, Issuer Scripting would normally be expected to occur after 2nd Card Action Analysis (i.e., a '72' command script).

Issuer Scripts are protected from alteration by the presence of a Message Authentication Code (MAC) generated by the Issuer.

17.2 Commands

The *Issuer Script Commands* to support these functions are:

- PUT DATA
- APPLICATION BLOCK
- PIN CHANGE/UNBLOCK
- APPLICATION UNBLOCK

Note that the Terminal processes the script commands as received in the Issuer's response message and passes them to the Card.

17.3 Processing Requirements

An AEIPS-compliant Terminal ***must*** support Issuer scripts labeled with either tag '71' or tag '72'.

The Terminal ***must*** submit Issuer scripts with tag '71' to the card for processing prior to issuing the final GENERATE AC command. Issuer scripts with tag '72' ***must*** be submitted after issuing the final GENERATE AC command.

Issuer Scripts ***must*** only be applied after the Chip Card has successfully performed Issuer Authentication.

It is ***mandatory*** that any Issuer Scripts received be processed as described in [EMV4.3iii] Sections 6, 10.10, and [EMV4.3iv] Section 6.3.9.

Although American Express only supports Issuer Scripts of tag '72', a terminal compliant with this manual ***must*** accept and process Issuer Scripts of both '71' and '72', should they be received. This means that a failure to process a script tag '71' would result in TVR byte 5 bit 6 being set to "1" although American Express does not support tag '71'. A failure to process tag '72' scripts results in the TVR byte 5 bit 5 being set to "1".

For details of how these secure messages are formatted see the American Express Chip Card Acquirer Guide [AG].

Issuer Scripts will only contain commands to be executed by the Chip Card. The only processing requirement of the Terminal is to extract the command or commands from the script or scripts in the order they are received in the authorization response message and to pass them to the Chip Card to be processed as per [EMV4.3iii] Section 10.10, then to check and report the results returned from the Chip Card.

17.4 Processing a Blocked Application

If the card application has been blocked using the APPLICATION BLOCK command in a script sent in a previous transaction, then the card behavior is altered such that a special transaction is required before an APPLICATION UNBLOCK command script can be forwarded by the terminal.

Similarly, for cards personalized such that the application is blocked if the PIN is blocked, or the PIN is blocked when the application is already blocked, then a similar procedure is required to unblock the PIN and application.

Support for the functionality supporting APPLICATION UNBLOCK and PIN UNBLOCK (when application blocked) is restricted to specific terminals, and is not a mandatory requirement. Terminals which support APPLICATION BLOCK and PIN UNBLOCK ***must*** allow for these features to be enabled or disabled through configuration. Local rules and conditions shall apply.

To support APPLICATION UNBLOCK and PIN UNBLOCK (when application blocked) the terminal ***must*** perform the following:

- Recognize that the application is blocked when receiving SW '6283' to the SELECT command and perform the following special processing.
- Continue the transaction and receive an AAC to the GENERATE AC.
- Send the transaction online to the Issuer.
- Receive the response and perform Issuer Authentication.
- If Issuer Authentication is successful, then send tag '72' received Issuer script commands to the Chip Card after the 2nd GENERATE AC (requesting AAC) for tag '72' script commands.
- The transaction is successful and the card and/or PIN unblocked when the terminal receives SW '9000' to the APPLICATION UNBLOCK and/or PIN UNBLOCK script command.

18 Transaction Completion

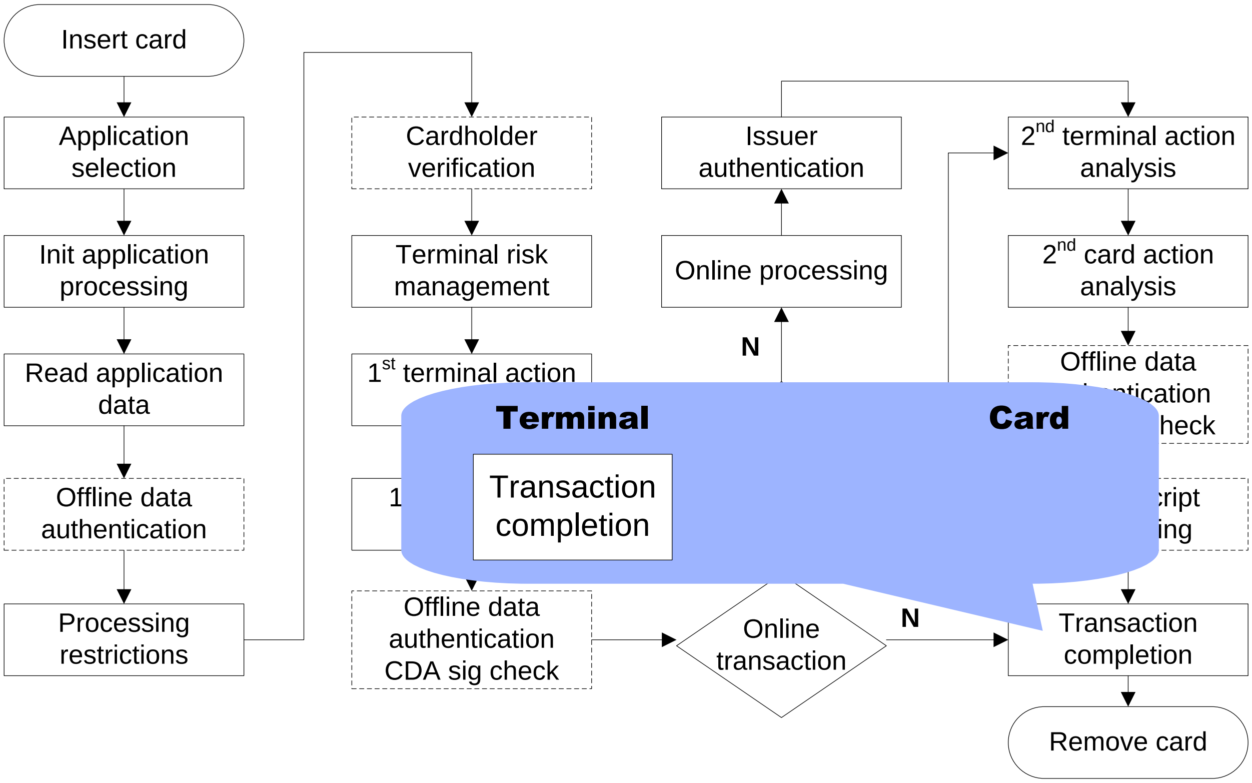

Figure 18-1: Transaction Completion Detail

18.1 Overview

The Terminal performs final processing to complete the transaction. If the Terminal transmits a clearing message subsequent to an authorization message, the TC is transmitted in the clearing message. With single message systems or systems involving Acquirer host data capture of approved transactions, the Terminal or Acquirer ***must*** generate a reversal for Issuer-approved transactions which are subsequently declined by the Chip Card.

American Express does not mandate anything beyond EMV and local market requirements for Transaction Completion.

Once the Chip Card has responded to the final GENERATE AC command, and any scripts have been processed, its role in the transaction is complete.

The Terminal will then perform any other functions required to complete the transaction. These include printing of receipts, obtaining a signature (where signature was the Cardholder Verification Method used) and storing the data for clearing.

18.2 Processing Requirements

18.2.1 Voice referrals

Transactions completed as voice referrals ***must*** complete as follows:

- If an AAC was requested to complete the transaction and the transaction approved, the ARQC ***must*** be submitted to the clearing and settlement system, and the AAC should be discarded
- If a TC was requested to complete the transaction and the transaction approved, the TC should be submitted.

19 Performance Requirements

There are no specific performance requirements for AEIPS Terminals.

20 Cryptographic Requirements

This section details the cryptographic security requirements to implement Chip Card payments as detailed in this manual. It is more technically detailed than other sections and is not intended for business readers.

20.1 Unpredictable Number Generation

The Terminal generates an *Unpredictable Number* (tag ‘9F37’) at the commencement of every transaction (i.e. as a result of the GET PROCESSING OPTIONS). The number is an essential security component preventing attacks on the payment system, such as pre-prepared *Application Cryptograms.*

American Express ***requires*** that the *Unpredictable Number* is unpredictable and not simply different for every transaction. Counters, repeating sequences or the results of simple logic (e.g. exclusive OR operations) are inadequate. Vendor’s attention is drawn to [EMV4.3iv] Section 6.5.6 and to EMV “Specification Bulletin 103” which provides notice that the *Unpredictable Number* is subject to further Type Approval.

20.2 Offline Data Authentication

Terminals ***must*** be capable of performing the cryptographic processes required to deliver Offline Data Authentication as described in Section 7 whilst meeting the performance requirements of Section 19. The processes are described in [EMV4.3ii] Sections 5 and 6, and [EMV4.3iii] Section 10.3.

Terminals ***must*** be able to store and use a minimum of six American Express CAPKs and associated data, as described in Section 7.3.1.

Currently, American Express does not support the use of Certificate Revocation Lists.

20.3 Offline PIN Encipherment

Terminals supporting Offline PIN CVM ***must*** be capable of processing Offline Enciphered PIN as described in Section 9.3 and in [EMV4.3ii] Section 7.

20.4 PIN Entry Device

If a PIN Pad is present, it ***must*** comply with EMV requirements as defined in [EMV4.3ii] Section 11.1, the PCI Security Standards Council PIN Transaction Security (PTS) requirements and guidelines and any additional local market requirements. American Express has no minimum requirements for PIN Pads above those of EMV, the PCI and the local market payment authorities or regulatory bodies.

21 Additional Product Specifics

21.1 Membership-Related Data Processing

21.1.1 Overview

The card issuer may require a unique Membership Reference Number or Membership Product or Scheme information be stored on the Card for processing at a Terminal that supports such a Membership scheme. To support this functionality the Card may hold optional data elements that provide values to support such Membership Related Data Processing.

During the Read Application Data phase of an AEIPS EMV transaction the Terminal may recover optional tags from the Card associated with a Membership Scheme by use of the READ RECORD command and reading the data elements from the data files that have been personalized on the Card during initial Card Issuance.

21.1.2 Data

The following data elements held on the Chip, are used by the Terminal:

- **Membership Product Identifier** – The presence of the Membership Product Identifier on the card is optional. The value of the field indicates which product (or 'scheme') is supported.
- **Product Membership Number** – the presence of the Product Membership Number on the card is optional. The field is dependent on a valid Membership Product Identifier being available. The value of the field, if present, indicates the membership number associated with the product.

The Membership Product Identifier indicates the Card is part of a membership scheme. The Product Membership Number optionally indicates the membership number for the membership scheme if required

Only one Membership Product Identifier and Product Membership Number pair may exist per Card.

21.1.3 Processing Requirements

The Terminal will read the membership details from the Card during Read Application Data processing using the READ RECORD commands. If the Terminal supports a membership scheme, then it may use the data in the Membership Product Identifier to identify whether the card is in a scheme that the Terminal supports. If the Terminal requires a Membership number associated with that scheme then the Terminal will use the Product Membership Number retrieved from the Card. The Terminal can then utilize these values to perform any Membership processing it requires. Any Membership Related Data processing must take place after the Read Application Data phase of the transaction and must not negatively impact the remainder of the AEIPS EMV Payment transaction flow, processing or performance.

The functionality to be performed as part of Membership Related Data is outside the scope of this Manual.

22 Data Elements

22.1 Data Overview

This section describes in detail all the data held and processed by an AEIPS-compliant payment application by looking at each group of data as described in Figure 22-1. It also describes the flexibility within which an AEIPS-compliant payment application can operate by identifying whether the presence of particular data items is ***mandatory*** (M), ***conditional*** (C) or ***optional*** (O). Any American Express restrictions on the values that particular data items can be assigned are also highlighted.

Figure 22-1 below identifies the different groups of data objects that may be found on an AEIPS-compliant Card. There card will contain at least one payment application. A Payment Systems Environment (PSE) may be present on the Chip Card in order to enable a Terminal to perform EMV processing more efficiently.

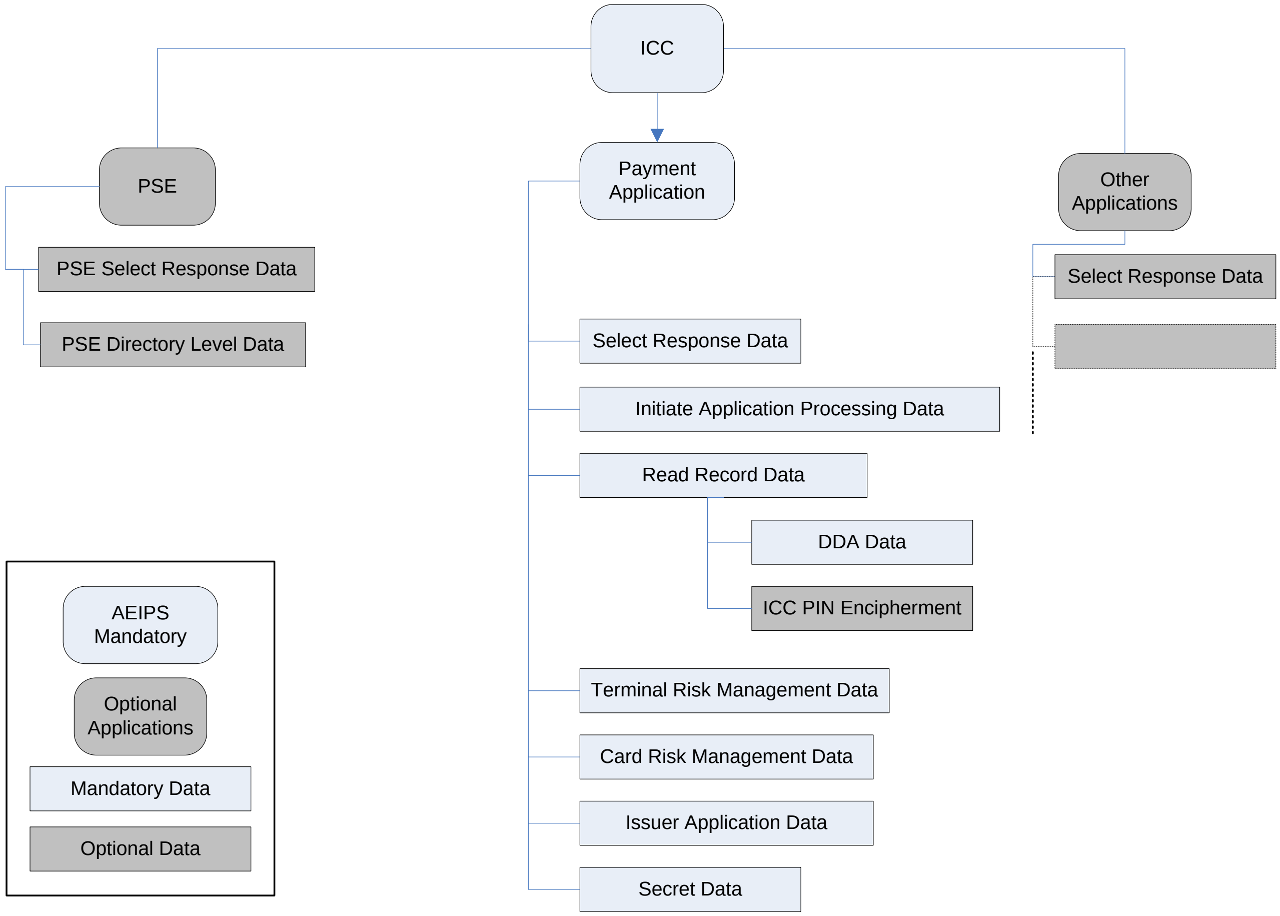

Figure 22-1: AEIPS Data

22.2 Payment Systems Environment

The presence of the PSE is ***optional***. However, the terminal ***must*** always support PSE processing (Section 4.3.3).

22.2.1 PSE Select Response Data

The PSE contains the following data objects as defined in [EMV4.3i] Sections 11.3.4 & 12.2.3 in the response to the SELECT command when the Payment System Environment (PSE) Directory is selected:

Table 22-1: PSE Response Data

Data Item			Presence	Value Restrictions
File Control Information (FCI) Template			M	
	Dedicated File (DF) Name		M	1PAY.SYS.DDF01
	FCI Proprietary Template		M	
		SFI of Directory Elementary File	M	This value must be in the range of 1-10 as specified by EMV.
		Language Preference	O	As defined in [ISO639]
		Issuer Code Table Index	C	As defined in [ISO8859]. ***Mandatory*** if Application Preferred Name is present.
		FCI Issuer Discretionary Data	O	As defined in [EMV4.3i] Section 11.3.4

The response data is returned as a nested Tag Length Value (TLV) structure, indicated by the shading in the table above. For more detail on the structure of response data to the SELECT ADF command, see [ISO7816-4].

22.2.2 PSE Directory Level Data

The data in Table 22-2 is stored in a payment system's directory elementary file retrievable by the READ RECORD command for use in application selection, as described in [EMV4.3i] Section 12 Application Selection.

To allow the support of multiple Application Identifiers within a single EMV payment application or function, the data in Application Template in Table 22-2 may appear several times in one or more records. See [EMV4.3i] Section 12.2.3.

Table 22-2: PSE Directory Level Data

Data Item			Presence
Application Elementary File (AEF) Data Template			M
	Application Template		M
		Application Definition File (ADF)	M
		Application Label	M
		Application Priority Indicator*	C
		Application Preferred Name	O

* Application Priority Indicator is ***mandatory*** if more than one application is personalized on the card.

22.3 Payment Application Data

The following subsections list the ***mandatory*** (M), ***conditional*** (C) and ***optional*** (O) data items that an AEIPS-compliant Chip Card stores and are used when the application is selected and an EMV transaction is performed.

22.3.1 Select Response Data

When the application to be used for this transaction has been chosen, the Terminal issues a SELECT ADF command for the ***required*** application.

In response to this command, the Chip Card returns the data elements detailed in Table 22-3.

Table 22-3: Select Response Data

Data Item			Presence	Value Restrictions
FCI Template			M	
	DF Name		M	
	FCI Proprietary Template		M	
		Application Label	M	The Application label *must* include a reference to American Express i.e. “AMEX” or “AMERICAN EXPRESS”.
		Application Priority Indicator	C	Though not a mandatory data element for all AEIPS-compliant Cards, this manual mandates the coding of the *Application Priority Indicator* when multiple Application Identifiers are supported. This allows the list of applications to be presented to the Cardholder for selection in a predefined order. Alternatively the Terminal may select the highest priority application supported by both Card and Terminal. See Table 22-4.
		PDOL	O	Defines data elements to be included in the command data of the GET PROCESSING OPTIONS command. May be necessary for some dual interface implementations. PDOL processing is described in Section 5.3.
		Language Preference	O	If language support is available on a payment Terminal, this option allows any customer display associated with the payment Terminal to display in the Card’s preferred language (as defined in [ISO639]).
		Issuer Code Table Index	C	If this data element is to be included, it ***must*** be coded according to [ISO8859]. The presence of this data element ***must*** be linked to the presence of the *Application Preferred Name*.
		Application Preferred Name	O	This field provides an alternative application name to the *Application Label* and allows the Application Name to be displayed by the Terminal in a preferred language. This field is linked to the Issuer Code Table Index.
		FCI Issuer Discretionary Data	O	As defined in [EMV4.3i] Section 11.3.4

The response data is returned as a nested Tag Length Value (TLV) structure, indicated by the shading in the table above. For more detail on the structure of response data to the SELECT ADF command, see [ISO7816-4].

Table 22-4: Application Priority Indicator (API)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X								1 = Cardholder confirmation required.
	0							RFU
		0						RFU
			0					RFU
				X	X	X	X	Order in which the application is to be listed or selected, ranging from 1 to 15, with 1 being the highest priority 0000 = no priority assigned
X = Configurable by Issuer, 1 or 0 = Mandatory value								

22.3.2 Initiate Application Processing Data

The GET PROCESSING OPTIONS command returns two data elements to the Terminal.

[EMV4.3iii] Section 6.5.8.4 Data returned in the response message, defines two possible formats for the GET PROCESSING OPTIONS response data. Currently this manual has no requirement to support additional data being returned during the GET PROCESSING OPTIONS command, therefore the data is returned in Format 1 as detailed in Table 22-5.

Table 22-5: Data Retrievable by Get Processing Options Command (GPO)

Data Item	Value Restrictions
Application Interchange Profile	The AIP specifies the application functions that are supported by the application in the Chip Card. See Table 22-6 for configuration options.
Application File Locator	The Application File Locator will be created as a result of the personalization of a Chip Card. The AFL indicates to the Terminal the data to be read using the READ RECORD command and which data records must be included in the Static Data Authentication process. See Table 22-23 for format and structure.

Table 22-6: Application Interchange Profile (AIP)

Byte 1 (leftmost)								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0								RFU
	X							1 = Static data authentication is supported 0 = Static data authentication is not supported
		X						1 = DDA is supported 0 = DDA is not supported*
			1					Cardholder verification is supported
				1				Terminal risk management is to be performed
					1			Issuer authentication is supported
						0		Reserved for use by the EMV Contactless Specifications
							X	1 = CDA is supported 0 = CDA is not supported*
X = Configurable by Issuer, 1 or 0 = Mandatory value								
Byte 2 (rightmost)								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning**
0								Reserved for use by the EMV Contactless Specifications
	0							Reserved for use by the EMV Contactless Specifications
		0						RFU by EMV Specifications
			0					RFU by EMV Specifications
				0				RFU by EMV Specifications
					0			RFU by EMV Specifications
						0		RFU by EMV Specifications
							0	RFU by EMV Specifications
X = Configurable by Issuer, 1 or 0 = Mandatory value								

22.3.3 Read Record Data

All data supplied to the Terminal for use in the processing of a financial transaction that is not dynamically maintained by the Chip Card will be held in file records and presented to the Terminal during the appropriate READ RECORD commands.

22.3.3.1 Read Record Data Objects

Table 22-7 lists the ***mandatory*** data objects that are always present in the responses to the READ RECORD command and are retrievable using the READ RECORD command as described in Section 6 using the Short File Identifiers (SFI) as provided in the AFL to identify the file in which the data objects are located.

Table 22-7: Read Record Data Objects

Data Item	Comments
Application Effective Date	A "YYMMDD" defined date indicating when this application is first valid is only checked by a Terminal. The results of this test are controlled by the Issuer Action Codes.
Application Expiration Date	A "YYMMDD" defined date indicating when this application is no longer valid is only checked by a Terminal. The results of this test are controlled by the Issuer Action Codes.
Application Primary Account Number	The account number associated with this application.
Application Version Number	Version number assigned by the Issuer for this application.
Application Usage Control	See Table 22-8
Cardholder Name	Var. 2-26
Card Risk Management Data Object List 1 (CDOL1)	See Table 22-9
Card Risk Management Data Object List 2 (CDOL2)	See Table 22-10
CVM List	American Express ***mandates***, independent of the card holder verification methods selected, the following CVM List priority order: - Enciphered PIN Verification online, if cash and the Terminal and application supports it. - Enciphered PIN Verification performed by Chip Card, if the Terminal and application supports it. - Plain text PIN Verification performed by Chip Card, if the Terminal and application supports it. - Signature, if the Terminal supports it. - No CVM required if not cash or cash back See Table 22-12 for details.
Issuer Action Code - Default	The Issuer Action codes are read by the Terminal for use in Terminal Action Analysis as defined in [EMV4.3iii] Section 10.7 Terminal Action Analysis.
Issuer Action Code - Denial	
Issuer Action Code - Online	
Issuer Country Code	Indicates the country of the Issuer, represented according to [ISO 3166].
PAN Sequence Number	Identifies and differentiates cards with the same PAN
Track 2 Equivalent Data	American Express ***mandates*** that Track 2 Equivalent Data be present in SFI 1 Record 1.

Table 22-8: Application Usage Control (AUC)

Byte 1 (leftmost)								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	Meaning
X								1 = Valid for Domestic Cash Transactions
	X							1 = Valid for International Cash Transactions
		X						1 = Valid for Domestic Goods
			X					1 = Valid for International Goods
				X				1 = Valid for Domestic Services
					X			1 = Valid for International Services
						X		1 = Valid at ATMs
							X	1 = Valid at Terminals other than ATMs
X = Configurable by Issuer, 1 or 0 = Mandatory value								
Byte 2 (rightmost)								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	Meaning
0								0 = Domestic Cashback not allowed
	0							0 = International Cashback not allowed
		0						RFU by EMV Specifications
			0					RFU by EMV Specifications
				0				RFU by EMV Specifications
					0			RFU by EMV Specifications
						0		RFU by EMV Specifications
							0	RFU by EMV Specifications
X = Configurable by Issuer, 1 or 0 = Mandatory value								
Note: The ISO Country Code of the Chip Card Issuer determines whether a transaction is domestic or international. If the ISO Country Code for the Chip Card and the terminal are the same, then the transaction is domestic. If the ISO Country Code in the terminal is different from the Chip Card, then the transaction is international.								

Table 22-9: CDOL1 Data Objects

Cryptogram Version Number	**Data Element**	**Tag**	**Length**
01	Amount, Authorized	'9F02'	6
	Amount, Other	'9F03'	6
	Terminal Country Code	'9F1A'	2
	Terminal Verification Results	'95'	5
	Transaction Currency Code	'5F2A'	2
	Transaction Date	'9A'	3
	Transaction Type	'9C'	1
	Unpredictable Number	'9F37'	4

Table 22-10: CDOL2 Data Objects

Cryptogram Version Number	Data Element	Tag	Length
01	Authorization Response Code	'8A'	2
	Amount, Authorized	'9F02'	6
	Amount, Other	'9F03'	6
	Terminal Country Code	'9F1A'	2
	Terminal Verification Results	'95'	5
	Transaction Currency Code	'5F2A'	2
	Transaction Date	'9A'	3
	Transaction Type	'9C'	1
	Unpredictable Number	'9F37'	4

Table 22-11: Authorization Response Code Values (Tag '8A')

Value	Meaning
00, 08, 10, 11	Card should treat this code as meaning an "Issuer approved transaction"
01, 02	Card should treat this code as meaning the "Issuer Requested Referral"
Other values	Card should treat this code as meaning the "Issuer has declined the transaction"
Z3	Value generated by the Terminal indicating to the card that the transaction was "Unable to go online (offline declined)"
Y3	Value generated by the Terminal indicating to the card that the transaction was "Unable to go online (offline approved)"

The *Authorization Response Code* is transmitted to the Chip Card in the 2nd GENERATE AC command data. It is either returned by the Issuer when the transaction has gone online, or if this was not possible, the Terminal generates it.

Table 22-12: Cardholder Verification Methods List

BYTE 1-4: Amount (“X”)	
BYTE 5-8: Amount (“Y”)	
BYTE 9: CVM Method Codes	
Bit Value	**Meaning**
bit 8: 0	RFU
bit 7: 0	Fail cardholder verification if this CVM is unsuccessful
bit 7: 1	Apply succeeding CVR field if this CVM is unsuccessful
bits 6-1: 000000	Fail CVM processing
bits 6-1: 000001	Plain Text PIN verification performed by ICC
bits 6-1: 000010	Enciphered PIN verified online
bits 6-1: 000011	Plain Text PIN performed by ICC and signature (paper)
bits 6-1: 000100	Enciphered PIN verification performed by ICC
bits 6-1: 000101	Enciphered PIN performed by ICC and signature (paper)
bits 6-1: 000110-011101	RFU
bits 6-1: 011110	Signature (paper)
bits 6-1: 011111	No CVM required
bits 6-1: 100000-101111	RFU by individual payment systems
bits 6-1: 110000-111110	RFU by Issuer
bits 6-1: 111111	Not Available For Use
BYTE 10: CVM Conditions	
Value	**Meaning**
‘00'	Always
‘01'	If unattended cash
‘02'	If not unattended cash, manual cash or purchase with cashback
‘03'	If terminal supports the CVM
‘04'	If manual cash
‘05'	If purchase with cashback
‘06'	If transaction is in Application Currency Code and is < X value
‘07'	If transaction is in Application Currency Code and is > X value
‘08'	If transaction is in Application Currency Code and is < Y value
‘09'	If transaction is in Application Currency Code and is > Y value
‘0A' – ‘7F’	RFU
‘80' – ‘FF’	Reserved for use by individual payment systems

Note: An additional 2 bytes are added following byte 10 for each additional CVM method code and corresponding CVM condition code.

22.3.3.2 Optional Read Record Data Objects

Table 22-13 lists the data objects defined in [EMV4.3iii] that may be present in READ RECORDs read by Terminals.

Table 22-13: Optional Data Objects

Data Item
Application Currency Code
Application Dual Currency Code
Application Discretionary Data
Cardholder Name – Extended
Membership Product Identifier
Product Membership Number
Service Code
Track 1 Discretionary Data
Track 2 Discretionary Data
Notes: If either the Amount "X" or Amount "Y" contained in the CVM List detailed in Table 22-12 is nonzero, or if the Offline Velocity Checks detailed in Section 12 and 16 are to be performed, the Application *Currency Code* ***must*** be present in the ICC. If *Product Membership Number* is to be present, then *Membership Product Identifier* ***must*** also be present.

22.3.4 SDA Data

In order to support SDA, Table 22-14 lists the data objects that may be present in the Chip Card for use in SDA processing. These data objects ***must*** be retrievable using the READ RECORD command as described in Section 6 using the SFI as provided in the AFL to identify the file in which the data objects are located.

If multiple application identifiers are to be included within a single application or payment function of the Chip Card, the data in Table 22-14 may appear several times to support each AID.

Table 22-14: Data used in Static Data Authentication

Data Item	Presence	Value Restrictions
Certification Authority Public Key Index	M	
Issuer Public Key Certificate	M	
Issuer Public Key Exponent	M	
Signed Static Application Data	M	The data objects used for signing will be retrievable by the Terminal using the READ RECORD command. American Express requires that the data objects shown in Table 22-15 be included within the Signed Static Application Data during card personalization.
Static Data Authentication Tag List	O	If present, the Static Data Authentication Tag List shall only contain the tag '82' identifying the AIP, and shall be used as defined in [EMV4.3ii], Section 5.1.1, "Static Data to be Authenticated".
Issuer Public Key Remainder	C	Issuer Public Key Remainder must be present if the length of the Issuer's Public Key (modulus) is greater than the Certification Authority Public Key minus 36 bytes.

Table 22-15 below details the data elements used to produce the Signed Application Data and written to the card at personalization for use in Offline Data Authentication as described in Section 7. In addition, the AIP is appended at the end of the data list, if the SDA taglist is present.

Table 22-15: Data Objects for Signing

Data Item
Application Effective Date
Application Expiration Date
Application Primary Account Number (PAN)
PAN Sequence Number
Issuer Action Code -Default
Issuer Action Code -Denial
Issuer Action Code -Online
Application Usage Control
Issuer Country Code
CVM List
AIP

22.3.5 DDA / CDA Data

The support for Dynamic Data Authentication (Standard DDA and CDA)is ***mandatory***. Table 22-16 lists the data objects that ***must*** be present for DDA are as stated in [EMV4.3ii] Section 6. These data objects ***must*** be retrievable using the READ RECORD command as described in Section 6, using the SFI as provided in the AFL to identify the file in which the data objects are located.

Table 22-16: Mandatory Data for Dynamic Data Authentication

Data Item	Presence	Value
Dynamic Data Authentication Data Object List (DDOL)	M	See Table 22-19
Application DDA Public Key Certificate	M	
Application DDA Public Key Exponent	M	
Application DDA Public Key Remainder	C	Application Public Key Remainder must be present if the length of the Application's Public Key (modulus) contained in the Card Signed Application Data is greater than the Certification Authority Public Key, minus 42 bytes.
Certification Authority Public Key Index	M	
Issuer Public Key Certificate	M	
Issuer Public Key Exponent	M	
Static Data to be Authenticated	M	The data objects shown in Table 22-18 used for signing will be retrievable by the Terminal using the READ RECORD command.
Static Data Authentication Tag List	O	If present, the Static Data Authentication Tag List ***must*** only contain the tag '82' identifying the AIP, and ***must*** be used as defined in [EMV4.3ii] Section 5.1.1 Static Data to be Authenticated.
Issuer Public Key Remainder	C	Issuer Public Key Remainder must be present if the length of the Issuer's Public Key (modulus) is greater than the Certification Authority Public Key minus 36 bytes.

American Express requires that the Public Key Modulus as stated in Table 22-17 ***must*** be supported by the Terminal, and that the DDOL contains data objects as stated in Table 22-19.

Table 22-17: Public key modulus lengths for which support is mandatory

Modulus	Length (bits)
Certification Authority Public Key Modulus	1408 and 1984
Issuer Public Key Modulus	1152,1408 and 1984
ICC Public Key Modulus	896, 1024 and 1152 and 1408

Table 22-18 below details the static data elements and if always present (i.e. M = Mandatory) or may be present (O=Optional). The AIP is appended at the end of the data list, if the Static Data Authentication Tag List is present.

Table 22-18: Static Data to be Authenticated

Data Item	Presence
Application Effective Date	M
Application Expiration Date	M
Application Primary Account Number (PAN)	M
PAN Sequence Number	M
Issuer Action Code -Default	M
Issuer Action Code -Denial	M
Issuer Action Code -Online	M
Application Usage Control	M
Issuer Country Code	M
CVM List	M
Membership Product Identifier	O
Product Membership Number	C
AIP	C

Table 22-19: DDOL Data Objects

Data Item	Presence
Terminal Country Code	O
Terminal Identification	O
Transaction Currency Code	O
Transaction Date	O
Transaction Type	O
Unpredictable Number	M

22.3.6 Chip Card PIN Encipherment Data

The support for an independent Chip Card PIN asymmetric key pair is ***optional***. If it is supported, Table 22-20 lists the additional data objects that are present. These data objects are retrieved using the READ RECORD command as described in Section 6 Read Application Data, using the SFI as provided in the AFL to identify the file in which the data objects are located.

Table 22-20: Mandatory Data for Chip Card PIN Encipherment

Data Item	Presence	Value
Application PIN Encipherment Public Key Certificate	M	
Application PIN Encipherment Public Key Exponent	M	
Application PIN Encipherment Public Key Remainder	C	Application Public Key Remainder ***must*** be present if the length of the Application's Public Key (modulus) contained in the Card Signed Application Data is greater than the Certification Authority Public Key, minus 42 bytes.

22.3.7 Terminal Risk Management Data

The data objects listed in Table 22-21 are not retrievable by the READ RECORD command as described in Section 6 Read Application Data, but may be retrieved by the Terminal using the GET DATA command as described in Section 10.

Table 22-21: Data Retrievable by GET DATA Command

Data Item
ATC
Last Online ATC Register
Remaining PIN Try Counter

The Terminal records the result of its risk management and action analysis in the TVR Data object, the meaning of which is detailed in Table 22-22. The TVR are included in both *CDOL1* (See Table 22-9) and *CDOL2* (See Table 22-10) and are therefore sent to the Chip Card as part of command data of the GENERATE AC command.

- If the transaction amount exceeds the Terminal Floor Limit then the Terminal sets the TVR byte 4 bit 8 to "1" as per [EMV4.3iii] Section 10.6.1.
- If velocity checking is performed and the check is exceeded then the Terminal shall set the TVR byte 4 bits 7 and 6 to "1" according to [EMV4.3iii] Section 10.6.3.

Table 22-22: Terminal Verification Results (TVR) Settings

Meaning	Byte	Bit(s)
Offline Data Authentication was not performed	1	8
Offline Static Data Authentication failed		7
Card Data Missing		6
Card appears on Terminal exception file		5
DDA failed		4
CDA failed		3
SDA selected		2
RFU		1
Card and Terminal have different application versions	2	8
Expired Application		7
Application not effective yet		6
Requested service not allowed for Card product		5
New Card		4
RFU		3 to 1
Cardholder Verification was not successful	3	8
Unrecognized CVM		7
Offline PIN Try Limit Exceeded		6
Offline PIN entry mandatory and PIN pad not present or not working		5
Offline PIN entry mandatory, PIN pad present, but PIN was not entered		4
Online PIN entered		3
RFU		2 to 1
Transaction Exceeds Floor Limit	4	8
Lower consecutive offline limit exceeded		7
Upper consecutive offline limit exceeded		6
Transaction selected randomly for online processing		5
Merchant forced transaction online		4
RFU		3 to 1
Default TDOL used (TDOL not supported in this manual)	5	8
Issuer Authentication was unsuccessful		7
Script processing failed before final GENERATE AC		6
Script processing failed after final GENERATE AC		5
RFU		4 to 1

22.4 Data Elements Table

This section defines those data elements that may be used for financial transaction interchange, and their mapping onto data elements. This section details the data elements directly relevant to implementing the AEIPS manuals and Expresspay specifications. For a full list of all EMV data elements see [EMV4.3iii] Annex A “Data Elements Dictionary”. The following abbreviations are used in this table (See [EMV4.3i] Section 4.3 for further details):

- a = Alpha
- an = Alphanumeric
- ans = Alphanumeric Special
- b = Binary
- cn = Compressed Numeric
- n = Numeric
- Var = Variable.

When the length defined for the data element is greater than the length of the actual data, the following rules apply:

- A data element in format ‘n’ is right-justified and padded with leading hexadecimal zeroes
- A data element in format ‘cn’ is left-justified and padded with trailing hexadecimal F
- A data element in format ‘an’ is left-justified and padded with trailing hexadecimal zeroes
- A data element in format ‘ans’ is left-justified and padded with trailing hexadecimal zeroes

Table 22-23: AEIPS Data Elements Table (DET)

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Additional Terminal Capabilities	Indicates the data input and output capabilities of the terminal.	Terminal	O	b	'9F40'	5	As per EMV	
Amount, Authorized (Numeric)	Authorized amount of the transaction (excluding adjustments).	Terminal	M	n 12	'9F02'	6		A ***mandatory*** data element the Terminal uses to populate a CDOL as read from the Card during Read Application Data.
Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cash back amount.	Terminal	M	n 12	'9F03'	6		A ***mandatory*** data elements the Terminal uses to populate a CDOL as read from the Card during Read Application Data.
Application Cryptogram (AC)	Application cryptogram computed by the Card during a transaction.	Card	M	b 64	'9F26'	8	Can be: ARQC AAC TC	This is a transient data element. Always returned to the Terminal in the response to the 1st GENERATE AC or 2nd GENERATE AC command.
Application Currency Code	Indicates the currency in which the account is managed.	Card	O	n 3	'9F42'	2	Coded according to [ISO4217]	If either the Amount “X” or Amount “Y” contained in the CVM List is nonzero or if the Offline Velocity Checks are to be performed, then this data element must be present in the Card. The data element is made available to the Terminal via the READ RECORD command.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Application DDA Public Key Certificate	Application DDA Public Key Certificate used during DDA process.	Card	C	b	'9F46'	Up to 176		Used for DDA/CDA. If DDA/CDA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bits 6 and 8 to “1” (ICC Data Missing and ODA Not Performed).
Application DDA Public Key Exponent	Exponent of Application DDA Public Key	Card	C	b	'9F47'	1 or 3		Used for DDA/CDA. If DDA/CDA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bits 6 and 8 to “1” (ICC Data Missing and ODA Not Performed).
Application DDA Public Key Remainder	Remaining digits of Application DDA Public Key.	Card	C	b	'9F48'	Var	See [EMV4.3ii], Section 6.1 Keys and Certificates. The *ICC Public Key Remainder* is equivalent to the *Application DDA Public Key Remainder* in this specification.	Used for DDA / CDA. If DDA/CDA is to be performed, Application Public Key Remainder ***must*** be present if the length of the Application’s Public Key (modulus) contained in the Card Signed Application Data is greater than the Issuer Public Key, minus 42 bytes. If it is required but missing, the Terminal must set the TVR byte 1 bits 6 and 8 to “1” (ICC Data Missing and ODA Not Performed).

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Application Definition File (ADF) Name	Identifies the name of the DF as associated with an application. See *Application Identifier (AID)*. Another name for the AID.	Card	M				See Application Identifier (AID)	Terminal must terminate the transaction if this data is missing.
Application Dual Currency Code	Indicates the currency in which the account is managed.	Card	O	n 3	'9F50'	2	Coded according to [ISO4217]	An ***optional*** data element made available to the Terminal via the READ RECORD command.
Application Discretionary Data	Issuer-specified data relating to the Card application.	Card	O	b 8-256	'9F05'	1-32		An ***optional*** data element made available to the Terminal via the READ RECORD command.
Application Effective Date	Date from which the Card application may be used.	Card	O	n 6 YYMMDD	'5F25'	3		An ***optional*** data element made available to the Terminal via the READ RECORD command.
Application Elementary File (AEF) Data Template	Indicates the record template of a record containing data elements. Templates are used to define TLV structures that contain other data elements.	Card	M	Var	'70'	Var		If the AEF is incorrectly formatted the Terminal must terminate the transaction.
Application Expiration Date	Date after which the Card application expires.	Card	M	n 6 YYMMDD	'5F24'	3		A ***mandatory*** data element made available to the Terminal via the READ RECORD command. Terminal must terminate the transaction if this data is missing.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Application File Locator (AFL)	Indicates the location (SFI, range of records) of the AEFs related to a given application.	Card	M	Var	'94'	Var up to 64	The AFL is made up of a number of 4 byte blocks of data (1 block per AEF), formatted as follows: Byte 1 (identifies AEF): Bits 8-4 = SFI Bits 3-1 = 000 Byte 2: First record number to be read for that SFI (never equal to zero) Byte 3: Last record number to be read for that SFI (***must*** be greater than or equal to byte 2) Byte 4: Number of consecutive records signed in *Signed Application Data*, starting with record number in byte 2 (may be equal to zero	This data element is always returned to the Terminal in a valid response to GET PROCESSING OPTIONS.
Application Identifier (AID) Terminal	Identifies the application as described in [ISO7816-4].	Terminal	M	b 40-128	'9F06'	5-16	Terminals enabled to accept the American Express payment application ***must*** be configured with an AID of A00000002501	Stored in the Terminal for use during application selection. Partial Application selection ***must*** be enabled for this AID.
Application Interchange Profile (AIP)	Indicates the capabilities of the Card to support specific functions in the application.	Card	M	b 16	'82'	2		A ***mandatory*** data element made available to the Terminal via the GET PROCESSING OPTIONS command. Terminal must terminate the transaction if this data is missing.
Application Label	Mnemonic associated with the AID.	Card	O	ans 1-16 (special character limited to space)	'50'	1-16	Used in application selection.	An ***optional*** data element returned in response to a SELECT command, providing a “friendly” name for an application.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Application PIN Encipherment Public Key Certificate	Application PIN Encipherment key certified by American Express.	Card	O	b	'9F2D'	Up to 176		Used for PIN Encipherment, if supported
Application PIN Encipherment Public Key Exponent	Exponent of Application PIN Encipherment Public Key.	Card	O	b	'9F2E'	1 or 3		Used for PIN Encipherment, if supported
Application PIN Encipherment Public Key Remainder	Remaining digits of Application PIN Encipherment Public Key.	Card	C	b	'9F2F'	Var	See [EMV4.3ii] Section 7.1 Keys and Certificates. The *ICC PIN Encipherment Public Key Remainder* is equivalent to the *Application PIN Encipherment Public Key Remainder* in [AEIPS-CARD].	Used for PIN Encipherment, if supported
Application Preferred Name	Preferred mnemonic associated with the Application Identifier of this application used by the Terminal in conjunction with the Issuer Code Table Index.	Card	O	ans 1-16 (special character limited to space)	'9F12'	1-16	Used in application selection to allow the *Application Label* to be displayed in an Issuer-defined language.	***Optional*** Data Element returned in response to a SELECT command.
Application Primary Account Number (PAN)	American Express Card number	Card	M	Var up to cn 19	'5A'	Var up to 10		A ***mandatory*** data element made available to the Terminal via the READ RECORD command. Terminal must terminate the transaction if this data is missing.
Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates Cards (Applications) with the same PAN.	Card	O	n 2	'5F34'	1		An ***optional*** data element made available to the Terminal via the READ RECORD command.
Application Priority Indicator	Indicates the priority of a given application or group of applications in a directory.	Card	O	b 8	'87'	1	See table 23-4 for potential settings for this data element.	***Optional*** Data Element returned in response to a SELECT command.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Application Transaction Counter (ATC)	Counter maintained by the application in the Card.	Card	M	b 16	'9F36'	2	Initial value is zero. It is incremented by 1 each time a transaction is performed.	Used by the Terminal during Terminal Risk Management. This data element is read only via the GET DATA command.
Application Usage Control	Indicates Issuer-specified restrictions on the geographic usage and services allowed for the Card application.	Card	O	b 16	'9F07'	2	Refer to table 23-8 for possible values of this data element.	An ***optional*** data element made available to the Terminal via the READ RECORD command.
Application Version Number	Version number assigned by the Issuer for the application.	Card	O	b 16	'9F08'	2		An ***optional*** data element made available to the Terminal via the READ RECORD command.
Application Version Number	Version number of a particular application supported by the Terminal	Terminal	M	b 16	'9F09'	2		It is ***mandatory*** that the Terminal store the application version number(s) that it supports for a given application.
Authorization Response Code (ARC)	Data Element generated by the Issuer Host System or the Terminal indicating the disposition of the transaction.	Issuer or Terminal	M	an 2	'8A'	2	Codes generated as indicated in table 23-11.	The value present forms part of the *Issuer Authentication Data* if received from the Issuer. The data is also sent to the Card as part of the 2nd GENERATE AC command forming part of the CDOL2.
Authorization Response Cryptogram (ARPC)	A cryptogram generated by the Issuer Host System during an online transaction	Issuer	M	B 64	—	8		A cryptogram generated by the Issuer Host System and included in the *Issuer Authentication Data* to be returned to the terminal and sent to the Chip Card in the response to an online transaction. Refer to *Issuer Authentication Data* in this table.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Card Risk Management Data Object list 1 (CDOL1)	List of data elements (tag and length) to be passed to the Card application with the 1st GENERATE AC command.	Card	M	b	'8C'	Var up to 64	See table 23-9.	A ***mandatory*** data element made available to the Terminal via the READ RECORD command. Terminal must terminate the transaction if this data is missing.
Card Risk Management Data Object List 2 (CDOL2)	List of data elements (tag and length) to be passed to the Card application with the 2nd GENERATE AC command.	Card	M	b	'8D'	Var up to 64	See table 23-10.	A ***mandatory*** data element made available to the Terminal via the READ RECORD command.
Cardholder Name	Indicates *Cardholder Name* according to [ISO7813].	Card	O	ans 2-26	'5F20'	2-26		An ***optional*** data element made available to the Terminal via the READ RECORD command.
Cardholder Name - Extended	Indicates the whole *Cardholder Name* when greater than 26 characters.	Card	O	ans 27-45	'9F0B'	27-45	According to [ISO 7813]	An ***optional*** data element made available to the Terminal via the READ RECORD command.
Cardholder Verification Method (CVM) List	Identifies a prioritized list of methods of verification of the Cardholder supported by the Card application.	Card	O	b	'8E'	Var up to 32	See table 23-12.	An ***optional*** data element made available to the Terminal via the READ RECORD command.
Cardholder Verification Method (CVM) List – Contactless	Identifies a prioritized list of methods of verification of the Cardholder supported by the Card application.	Card	M	b	'9F6F'	Var up to 32		A data element made available to the Terminal via the READ RECORD command for contactless interface. This tag is only used for scripting routing purposes. When personalized it will be used as “8E”

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
CDA Mode	Configuration parameter defining which of the four possible CDA Modes to apply when Terminal requests an ARQC during 1st GENERATE AC as defined by [EMV4.3ii] Annex D4.	Terminal	M	b	—	Var	As defined by Terminal configuration management	Configured into Terminal from Terminal Management System or equivalent.
Certification Authority Public Key Checksum	A check value calculated on the concatenation of the following parts of the Certification Authority Public Key (RID, *Certification Authority Public Key Index*, *Certification Authority Public Key Modulus*, *Certification Authority Public Key Exponent*) using SHA-1.	Terminal	C	b	—	20	Var	Used for Offline Data Authentication (ODA) . If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to “1” (ODA Not Performed).
Certification Authority Public Key Exponent	Value of the exponent part of the Certification Authority Public Key.	Terminal	C	b	—	1 or 3	Key length selected by Issuer. Values assigned by American Express.	Used for Offline Data Authentication (ODA) . If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to “1” (ODA Not Performed).
Certification Authority Public Key Index	Identifies the certification authority’s public key in conjunction with the Registered Identification Provider (RID) for use in static data authentication.	Card	C	b 8	'8F'	1	Key length selected by Issuer. Values assigned by American Express.	Used for Offline Data Authentication (ODA) . If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to “1” (ODA Not Performed).

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Certification Authority Public Key Modulus	Value of the Modulus part of the Certification Authority Public Key.	Terminal	C	b	—	Up to 248	Key length selected by Issuer. Values assigned by American Express.	Used for Offline Data Authentication (ODA) . If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to “1” (ODA Not Performed).
Cryptogram Information Data	Indicates the type of cryptogram (TC, ARQC or AAC) returned by the Card and the actions to be performed by the Terminal.	Card	M	b 8	'9F27'	1	Bits 8-7: 00 = AAC 01 = TC 10 = ARQC 11 = RFU Bit 6-5: RFU Bit 4: 1 = Advice required Bits 3-1 (Reason/Advice/ Referral Code): 000 = No information given 001 = Service not allowed 010 = *PIN Try Limit* exceeded 011 = Issuer authentication failed 1xx = RFU	This is information the application returns to the Terminal indicating the type of AC being sent. It is generated dynamically and not subsequently stored within the application. Always present in a valid response to the GENERATE AC command.
Default Dynamic Data Authentication Data Object List (DDOL)	DDOL to be used by the Terminal in the construction of the Internal Authenticate command if no DDOL is present in the card	Terminal	M	b	—	Var up to 32		A ***mandatory*** data element in DDA supporting terminals.
Dynamic Data Authentication Data Object List (DDOL)	List of data elements (tag and length) to be passed to the Card when the Card and the Terminal are performing DDA / CDA.	Card	O	b	'9F49'	Var up to 32		Available to Terminal via READ RECORD command.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
File Control Information (FCI) Issuer Discretionary Data	1 or more additional proprietary data elements from an application provider, Issuer, or IC card supplier, or EMV-defined tags that are specifically allocated to 'BF0C'	Card	M	Var	'BF0C'	Var up to 222		If the FCI is incorrectly formatted the Terminal ***must*** terminate the transaction.
File Control Information (FCI) Proprietary Template	Identifies the data elements proprietary to the [EMV 4.2i] in the FCI Template.	Card	M	Var	'A5'	Var	As defined in [EMV 4.2i]	***Mandatory*** Data Element returned in response to a SELECT command. If the FCI is incorrectly formatted the Terminal ***must*** terminate the transaction.
File Control Information (FCI) Template	Identifies the FCI template.	Card	M	Var	'6F'	Var up to 64		***Mandatory*** Data Element returned in response to a SELECT command. If the FCI is incorrectly formatted the Terminal ***must*** terminate the transaction.
ICC Dynamic Number	Time-variant number generated by the Card, to be captured by the Terminal.	Card	C	b	'9F4C'	8		This is a transient Data element generated By the card for use in Offline Data Authentication (see [AEIPS-CARD] Section 7.3).
Issuer Action Code - Default	Specifies conditions that cause a transaction to be declined if it might have been approved online, but the Terminal is unable to process the transaction online.	Card	O	b 40	'9F0D'	5		A data element made available to the Terminal via the READ RECORD command and used during Terminal Action Analysis to modify the Terminal Action Code setting.
Issuer Action Code - Denial	Specifies conditions that cause the decline of a transaction without attempting to go online.	Card	O	b 40	'9F0E'	5		A data element made available to the Terminal via the READ RECORD command and used during Terminal Action Analysis to modify the Terminal Action Code setting.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Issuer Action Code - Online	Specifies conditions that cause a transaction to be transmitted online.	Card	O	b 40	'9F0F'	5		A data element made available to the Terminal via the READ RECORD command and used during Terminal Action Analysis to modify the Terminal Action Code setting.
Issuer Application Data	Contains proprietary application data for transmission to American Express in all transaction messages.	Card	O	b	'9F10'	Var 32	The first byte indicates the length of the discretionary data. In this specification, the discretionary data is 6 bytes long: • Derivation Key Index (1 byte) • Cryptogram Version Number (1 byte) • Card Verification Results (4 bytes)	This is a transient data element that is constructed by concatenating other data elements as indicated.
Issuer Authentication Data	Issuer data transmitted to Card for online Issuer authentication.	Issuer	O	b 64-128	'91'	Up to 16	The *Issuer Authentication Data* consists of the following data: • First 8 bytes=ARPC • Last 2 bytes= Authorization Response Code	This data is transmitted to the Card by the Terminal in the EXTERNAL AUTHENTICATE command when performing Issuer Authentication.
Issuer Code Table Index	Indicates the code table to be used for displaying the *Application Preferred Name* at the Terminal.	Card	O	n 2	'9F11'	1	According to [ISO 8859]	***Optional*** Data Element returned in response to a SELECT command.
Issuer Country Code	Indicates the country of the Issuer, represented according to [ISO 3166].	Card	O	n 3	'5F28'	2	According to [ISO 3166]	An ***optional*** data element made available to the Terminal via the READ RECORD command, used when present, during Processing Restrictions.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Issuer Public Key Certificate	Issuer's public key certified by a certification authority for use in static data authentication.	Card	C	b 512-1984	'90'	Var 64-248		Used for Offline Data Authentication (ODA). If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to "1" (ODA Not Performed).
Issuer Public Key Exponent	Issuer-specified data to be used with the Issuer's public key algorithm for static data authentication.	Card	C	b	'9F32'	1 or 3		Used for Offline Data Authentication (ODA). If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory***. If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to "1" (ODA Not Performed).
Issuer Public Key Remainder	Remaining digits of the Issuer's public key to be hashed.	Card	C	b	'92'	Var	See [EMV4.3ii], Sections 5.1 & 6.1 Keys and Certificates.	Used for Offline Data Authentication (ODA). If ODA is to be performed (indicated by AIP and supported by Terminal) then this field is ***mandatory*** if the length of the Issuer Public Key Modulus is greater than (the length in bytes of the Certification Authority Public Key Modulus minus 36). If it is required but missing, the Terminal must set the TVR byte 1 bit 8 to "1" (ODA Not Performed).

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Issuer Script Template ‘71’	Contains proprietary Issuer data for transmission to the Card after the 2nd GENERATE AC command.	Issuer	O	b	'71'	Var		Although not supported by American Express Issuers Terminals are expected to process the templates safely and accurately. This information is processed by ISSUER SCRIPT PROCESSING and not subsequently stored within an application on the Card.
Issuer Script Template ‘72’	Contains proprietary Issuer data for transmission to the Card after the 2nd GENERATE AC command.	Issuer	O	b	'72'	Var		This information is processed by ISSUER SCRIPT PROCESSING and not subsequently stored within an application on the Card.
Language Preference	Table of up to four language codes indicating the preferred language for Terminal messages to be displayed to the Cardholder.	Card	O	an 2	'5F2D'	2-8	[ISO639] codes alpha-numeric codes	Data element returned in response to an APPLICATION SELECT command.
Last Online ATC Register	ATC value of the last transaction that went online.	Card	O	b 16	'9F13'	2	Initial value is zero. Updated to contain the current value of the ATC when a transaction has been transmitted online and Issuer Authentication is successful.	Data item used by Terminal Risk Management, retrievable via the GET DATA command.
Maximum Target Percentage to be Used for Biased Random Selection	Value used in Terminal Risk Management for random transaction selection.	Terminal	O	—	—	—	00-99	
Membership Product Identifier	A product identifier for the membership scheme.	Card	O	an	'9F5A’	Var up to 8		An ***optional*** data element used by the Terminal to determine whether card is in a supported membership scheme.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Merchant Category Code	Classifies the type of business done by the merchant.	Terminal	M	n 4	'9F15'	Var up to 15	As per [ISO8583] for Card Acceptor Business Code.	
Merchant Identifier	When concatenated with the Acquirer Identifier, uniquely identifies a given merchant	Terminal	M	ans 15	'9F16'	Var up to 15	Var	
Merchant Name Location	Indicates the name and location of the merchant	Terminal	M	ans	—	Var	Var	
Point of Service (POS) Entry Mode	Indicates source of Cardholder account data.	Terminal	M	n 2	'9F39'	1	According to [ISO 8583]	
Processing Options Data Object List (PDOL)	Contains a list of terminal resident data elements (tags and lengths) needed by the ICC in processing the GET PROCESSING OPTIONS command	Card	O	B	'9F38'	Var		May be necessary for some Dual Interface Implementations
Product Membership Number	A unique number to identify the cardholder as part of the scheme.	Card	C	an	‘9F5B’	Var up to 32		An ***optional*** data element whose presence is ***conditional*** on tag ‘9F5A’ being present. It is used by the Terminal to uniquely identify the cardholder as being part of the membership scheme.
Registered Application Provider Identifier (RID)	First 5 bytes of an AID registered as owned by the Card Scheme or Card Issuer.	Terminal	M	B	—	5	The value assigned to American Express is A000000025.	
Remaining PIN Try Counter	Indicates the remaining PIN attempts. Can be used by the Terminal during offline PIN processing.	Card	C	B	'9F17'	1		A ***conditional*** Data element ***mandatory*** if a *Reference PIN* is present. Used in Terminal Risk Management retrievable using the GET DATA command.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Response Message Template Format 1	Contains the data elements (without tags and lengths) returned by the Card in response to a GET PROCESSING OPTION, or a GENERATE AC without signature command.	Card	O	Var	'80'	—	Var	See [AEIPS-CARD] Section 5 “Initiate Application Processing”.
Response Message Template Format 2	Contains the data elements (with tags and lengths) returned by the Card in response to a GENERATE AC with signature command.	Card	O	Var	'77'	—	Var	Used if the response is being returned in a signature as specified for the CDA function.
Service Code	*Service Code* as defined on magnetic stripe tracks 1 and 2.	Card	O	n 3	'5F30'	2	Should match the value on the Card magstripe (if present) and be coded according to [ISO7813].	An ***optional*** data element retrievable via the READ RECORD command.
Short File Identifier (SFI)	Identifies the SFI to be used in the commands related to a given AEF.	Card	M	b 8	'88'	1	Values are 1-10: Governed by joint payment systems11-20: American Express specific 21-30: Issuer Specific	SFIs are pointers contained in a valid response to the SELECT command to the records readable during READ APPLICATION DATA.
Static Data Authentication Tag List	List of Tags of primitive data elements defined in [EMV4.3iii] whose value fields are to be included in the signed static or dynamic application data.	Card	O	—	'9F4A'	Var	Tag 82 (Application Interchange Profile)	A data element made available to the Terminal via the READ RECORD command.
Target Percentage to be Used for Random Selection	Value used in terminal risk management for random transaction selection.	Terminal	O	—	—	—	00-99	

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Terminal Action Code - Default	Specifies the Acquirer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online.	Terminal	M	b 40		5		Used along with Issuer Action Codes, to decide on action to be taken during Terminal Action Analysis.
Terminal Action Code - Denial	Specifies the Acquirer's conditions that cause a transaction to be denied without an attempt to go online.	Terminal	M	b 40		5		Used along with Issuer Action Codes, to decide on action to be taken during Terminal Action Analysis.
Terminal Action Code - Online	Specifies the Acquirer's conditions that cause a transaction to be transmitted online.	Terminal	M	b 40		5		Used along with Issuer Action Codes, to decide on action to be taken during Terminal Action Analysis
Terminal Capabilities	Indicates the Card data input, CVM, and security capabilities of the terminal.	Terminal	M	B	'9F33'	3	As per EMV	
Terminal Country Code	Indicates the country of the Terminal represented according to [ISO3166].	Terminal	M	n 3	'9F1A'	2		A ***mandatory*** data element. It is one of the data elements the Terminal uses to populate a CDOL.
Terminal Floor Limit	Indicates the Floor limit in the terminal in conjunction with the AID.	Terminal	O	B	'9F1B'	4	Var	The amount above which, all transactions are attempted online.
Terminal Identification	Designates the unique location of a Terminal at a merchant.	Terminal	O	an 8	'9F1C'	8	Var	
Terminal Type	Indicates the Environment of the Terminal, its communication capability, and its operational control.	Terminal	M	n 2	'9F35'	1	As per EMV	A ***mandatory*** data element. It is one of the data elements the Terminal uses to populate a CDOL.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Terminal Verification Results	Status of the different functions as seen from the Terminal.	Terminal	M	b 40	'95'	5	See table 23-20 for possible values.	A ***mandatory*** data element. It is one of the data elements the Terminal uses to populate a CDOL.
Threshold Value for Biased Random Selection	Value used in Terminal Risk Management for random transaction selection.	Terminal	O	—	—	—	***Must*** be 0 or a value less than the *Terminal Floor Limit*	
Track 1 Discretionary Data	Discretionary data associated with the magnetic stripe track 1.	Card	O	ans	'9F1F'	Var up to 16	Coded according to [ISO7813]	***Optional*** data element available via READ RECORD command.
Track 2 Discretionary Data	Discretionary data associated with the magnetic stripe track 2.	Card	O	cn	'9F20'	Var	Coded according to [ISO7813].	***Optional*** data element available via READ RECORD command.
Track 2 Equivalent Data	Image of magnetic stripe Track 2.	Card	M	cn	'57'	Var up to 19	According to [ISO7813]	***Mandatory*** data element available via READ RECORD command ***must*** be present in SFI 1 Record 1.
Transaction Amount	Clearing amount of the transaction, including tips and other adjustments	Terminal	M	n 12	—	6		
Transaction Currency Code	Indicates the currency code of the transaction according to [ISO4217]. The implied exponent is indicated by the minor unit of currency associated with the *Transaction Currency Code* in [ISO4217].	Terminal	M	n 3	'5F2A'	2		A ***mandatory*** data element. It is one of the data elements the Terminal uses to populate a CDOL.
Transaction Currency Exponent	Indicates the implied position of the decimal point from the right of the transaction amount.	Terminal	O	n 1	'5F36'	2	According to [ISO4217]	
Transaction Date	Local date that the transaction was attempted.	Terminal	M	n 6 YYMMDD	'9A'	3		A ***mandatory*** data element. It is one of the data elements the Terminal uses to populate a CDOL.

Name	Description	Source	Presence	Format	Tag	Length	Values	Location/Usage
Transaction Type	Indicates the type of financial transaction, represented by the first two digits of [ISO8583] Processing Code. The actual values to be used for the Transaction Type data element are defined by the relevant payment system.	Terminal	M	n 2	'9C'	1		A ***mandatory*** data element. It is one of the data elements the Terminal uses to populate a CDOL.
Transaction Personal Identification Number (PIN) Data	Data entered by the Cardholder to verify a PIN offline.	Terminal	C	B	'99'	8	Var	A ***conditional*** data element which ***must*** be present for Offline PIN.
Transaction Sequence Counter	Counter maintained by the terminal that is incremented by one for each transaction.	Terminal	M	n 4-8	'9F41'	2-4	Var	
Transaction Status Information (TSI)	Indicates the function performed in a Transaction	Terminal	M	B	'9B'	2		Set by the Terminal during the transaction as defined in EMV 4.2. Proper setting of TSI is a Level II EMV certification requirement.
Transaction Time	Local time that the transaction was attempted	Terminal	M	n 6 HHMMSS	'9F21'	3	Var	
Unpredictable Number	Value to provide variability and uniqueness to the generation of the application cryptogram.	Terminal	M	b 32	'9F37'	4		This is passes to the Card application by the Terminal and used within the GENERATE AC process.

23 Glossary

Table 23-1: Acronyms and Abbreviations

Term	Description
AAC	Application Authentication Cryptogram
AC	Application Cryptogram
ADF	Application Directory File
AEF	Application Elementary File
AEIPS	American Express ICC Payment Manual (Terminal and Chip Card)
AFL	Application File Locator
AID	Application Identifier as defined in [ISO/IEC7816-4]
AIP	Application Interchange Profile
APDU	Application Protocol Data Unit. The unit of information passed between a Terminal and a Smart Card according to [ISO7816].
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
CA	Certification Authority
Cardholder	American Express Cardmember
CDA	Combined Dynamic Data Authentication / AC Generation
CDOL	Card Risk Management Data Object List
CVM	Cardholder Verification Method
CVR	Cardholder Verification Results
DDA	Dynamic Data Authentication
DDF	Directory Definition File
DDOL	Dynamic Authentication Data Object List
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DET	Data Element Table

Term	Description
DF	Dedicated File
Disposition	The transaction outcome that Terminal processing indicates is preferable at a particular point during the transaction (e.g., if the Terminal disposition is for an offline approval it will request a TC when it issues a 1st GENERATE AC).
EMV	Europay, MasterCard and Visa. A term that is used to refer to the specifications developed by these three bodies.
FCI	File Control Information
Financial Transaction	The set of command-response pairs that are used to satisfy the payment business function.
IAC	Issuer Action Code
IC	Integrated Circuit. Component of the ‘Smart Card’.
ICC	Integrated Circuit Card. Synonymous with ‘Smart Card’ and ‘Chip Card’.
IFD	Interface Device
Issuer	An organization which prepares the application, establishes its processing options and cryptographic keys, provides online transaction authorization, and can modify the application after it has been issued.
Issuer Script	A set of commands sent from the Issuer to the application, which can modify the application’s data or status.
MAC	Message Authentication Code. A short digest, which is representative of a (usually longer) message. It may accompany the message, and may be used by a recipient to verify the integrity of the message.
PAN	Primary Account Number
Payment Application	Depending on the context. This is the AEIPS-compliant payment functionality on a Smart Card which may support a payment account.
PDOL	Processing Options Data Object List
PIN	Personal Identification Number
Primitive Data Object	Data returned or sent to the Card which includes the TLV of the data item concerned.
PSE	Payment Systems Environment
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
RSA	Rivest, Shamir and Adleman. Inventors of the RSA public key algorithm.
SDA	Static Data Authentication

Term	Description
SFI	Short File Identifier [ISO7816-4]
SHA-1	Secure Hash Algorithm 1
SW1	Status Word byte 1 [ISO7816-4]
SW2	Status Word byte 2 [ISO7816-4]
TC	Transaction Certificate
TLV	Tag, Length, Value
TVR	Terminal Verification Results

24 Index

1

1st Card Action Analysis 16, 43, 44, 45
1st Terminal Action Analysis.................................. 16, 40, 42

2

2nd Card Action Analysis 16, 52, 53, 54
2nd Terminal Action Analysis 16, 50

A

AAC.. 40, 44, 47, 50, 52, 55, 57
Abbreviations.. 94
Acronyms... 94
Advice Messages 51
Application Authentication Cryptogram 40, 41, 42, 94
Application Cryptogram................. 28, 40, 42, 50, 52, 54, 59
Application File Locator 22, 64, 94
Application Interchange Profile 22, 64, 65, 94
Application Selection........................... 15, 19, 20, 21, 23, 62
Application Usage Control.................... 15, 31, 32, 66, 67, 72
ARPC.. 46, 48, 94
ARQC 30, 40, 46, 50, 52, 57, 94
ATC 39, 73, 94
Authorization Response Code......... 41, 42, 47, 48, 50, 51, 68
Authorization Response Cryptogram 46, 48, 94

C

Card Risk Management.................................... 42, 44, 66, 94
Cardholder Verification 15, 33, 40
Cardholder Verification Method 33, 34, 36, 37, 57, 69
CDA...................26, 28, 29, 30, 43, 45, 51, 53, 65, 71, 74, 94
CVM 33, 35, 36, 37, 59, 66, 69, 70, 72, 74

D

Data Elements 61, 75, 76

E

EXTERNAL AUTHENTICATE 16, 46, 48, 49

G

GENERATE AC.....16, 30, 41, 42, 45, 47, 50, 52, 55, 57, 68, 73, 93
GET DATA.. 16, 33, 36, 38, 39, 73
GET PROCESSING OPTIONS...... 16, 22, 23, 34, 59, 63, 64

I

Initiate Application Processing 15, 22, 23, 64
Issuer Action Codes 32, 38, 40, 41, 42, 47, 51, 66
Issuer Authentication 16, 46, 47, 48, 49, 50, 51, 52, 55, 74
Issuer Authentication Data.......................... 46, 48, 49, 50, 51
Issuer Script Processing 16, 54

O

Offline Data Authentication15, 24, 26, 28, 29, 30, 40, 45, 59, 74
Offline Processing.. 41
Online Processing 16, 44, 46, 48, 49, 50, 54

P

Performance Requirements 58
Processing Restrictions 15, 31, 40

R

Read Application Data 15, 23, 24, 28, 31, 41, 60
READ RECORD 17, 19, 24, 28, 60, 62, 64, 65, 66, 70, 71, 73, 80, 85, 90

S

SDA 15, 26, 27, 28, 29, 96
SELECT.................................. 17, 19, 21, 55, 61, 62, 63, 79
Static Data Authentication 26, 27, 29, 64, 71, 72, 74, 96

T

TC 30, 40, 42, 44, 45, 47, 50, 51, 52, 53, 57, 95, 96
Terminal Action Codes 32, 38, 40, 41, 42, 51
Terminal Risk Management.................. 16, 38, 39, 40, 41, 73
Terminal Verification Results 25, 35, 38, 67, 68, 74, 96
Transaction Completion... 16, 44, 57

U

Unpredictable Number................................ 30, 59, 67, 68, 72