Welcome to

Visa Integrated Circuit Card Specification

The *Visa Integrated Circuit Card (ICC) Specification* has been updated. Please see the Chapter 1, Section 1.6, "Impact Summary" for information on what has changed from Visa ICC Specification (VIS) version 1.3.2.

This document is the final copy of the Visa ICC Specification version 1.4.0. It reflects changes from the copy published on the Visa website in April 2001. These changes are noted in a separate changes list available on the Visa website. It is important that Visa staff, members, and vendors review the changes list.

If you have any comments regarding this manual, please contact your regional representative. Your opinion is important to us.

Effective: 31 October 2001

Visa Integrated Circuit Card

Card Specification
Version 1.4.0

Effective: 31 October 2001

Printed on recycled paper.

Contents

Chapter 1 • About This Specification

1.1 Audience 1–2

1.2 VIS Update 1–2

1.3 Terminology 1–3

1.3.1 Mandatory/Required/Recommended/Optional 1–3

1.3.2 Card/Integrated Circuit 1–3

1.3.3 Terminated Transactions 1–3

1.4 Document Structure 1–4

1.4.1 Volume Overview 1–4

1.4.2 Chapter Overview 1–4

1.4.3 Subheading Overview 1–6

1.5 Revisions to This Specification 1–7

1.6 Impact Summary 1–7

1.6.1 Terminal 1–7

1.6.1.1 Mandatory 1–7

1.6.1.2 Optional 1–8

1.6.2 Card 1–8

1.6.2.1 Mandatory 1–8

1.6.2.2 Optional 1–9

1.7 Reference Materials 1–10
1.7.1 International Organisation for Standardisation (ISO) Documents 1–10
1.7.2 EMV Documents 1–11
1.7.3 Visa Documents 1–11

Chapter 2 • Processing Overview

2.1 Functional Overview 2–1
2.1.1 Application Selection (mandatory) 2–1
2.1.2 Initiate Application Processing/Read Application Data (mandatory) 2–2
2.1.3 Offline Data Authentication 2–2
2.1.4 Processing Restrictions (mandatory) 2–3
2.1.5 Cardholder Verification (mandatory) 2–3
2.1.6 Terminal Risk Management (mandatory) 2–3
2.1.7 Terminal Action Analysis (mandatory) 2–4
2.1.8 Card Action Analysis (mandatory) 2–4
2.1.9 Online Processing 2–5
2.1.10 Issuer-to-Card Script Processing 2–5
2.1.11 Completion (mandatory) 2–6
2.2 Mandatory and Optional Functionality 2–8
2.2.1 Card Functional Requirements 2–8
2.2.2 Command Support Requirements 2–10

Chapter 3 • Application Selection

3.1 Card Data 3–2
3.2 Terminal Data 3–5
3.3 Commands 3–6
3.4 Building the Candidate List 3–7
3.4.1 Directory Selection Method 3–7
3.4.2 List of AIDs Method 3–10

3.5 Identifying and Selecting the Application 3–11
3.6 Flow 3–12
3.7 Subsequent Related Processing 3–14

Chapter 4 • Initiate Application Processing

4.1 Card Data 4–2
4.2 Terminal Data 4–3
4.3 GET PROCESSING OPTIONS Command 4–4
4.4 Processing 4–4
4.5 Prior Related Processing 4–7
4.6 Subsequent Related Processing 4–7

Chapter 5 • Read Application Data

5.1 Card Data 5–2
5.2 Terminal Data 5–3
5.3 READ RECORD Command 5–3
5.4 Processing 5–3
5.5 Prior Related Processing 5–3
5.6 Subsequent Related Processing 5–3

Chapter 6 • Offline Data Authentication

6.1 Keys and Certificates 6–3
6.1.1 Visa Certificate Authority (CA) 6–3
6.1.2 RSA Key Pairs 6–3
6.1.2.1 Visa Public/Private Keys 6–3
6.1.2.2 Issuer Public/Private Keys 6–4
6.1.2.3 ICC Public/Private Keys 6–5

6.2 Determining Whether to Perform SDA or DDA 6–6
6.2.1 Card Data 6–6
6.2.2 Processing 6–6
6.3 Static Data Authentication (SDA) 6–7
6.3.1 Card Data 6–7
6.3.2 Terminal Data 6–9
6.3.3 Commands 6–9
6.3.4 Processing 6–9
6.4 Dynamic Data Authentication (DDA) 6–10
6.4.1 Card Data 6–11
6.4.2 Terminal Data 6–13
6.4.3 Commands 6–13
6.4.3.1 INTERNAL AUTHENTICATE Command 6–13
6.4.3.2 GENERATE APPLICATION CRYPTOGRAM (AC) Command 6–13
6.4.4 Processing 6–14
6.4.4.1 Standard DDA 6–14
6.4.4.2 Combined DDA/AC Generation 6–16
6.5 Prior Related Processing 6–16
6.6 Subsequent Related Processing 6–17

Chapter 7 • Processing Restrictions

7.1 Card Data 7–2
7.2 Terminal Data 7–3
7.3 Processing 7–3
7.3.1 Application Version Number 7–3
7.3.2 Application Usage Control 7–4
7.3.3 Application Effective Date 7–5
7.3.4 Application Expiration Date 7–6

7.4 Prior Related Processing 7–6
7.5 Subsequent Related Processing 7–6

Chapter 8 • Cardholder Verification

8.1 Card Data 8–2
8.2 Terminal Data 8–8
8.3 Commands 8–8
8.4 Processing 8–9
8.4.1 CVM List Processing 8–9
8.4.2 Offline PIN Processing 8–9
8.4.3 Processing of Other CVMs 8–14
8.5 Prior Related Processing 8–14
8.6 Subsequent Related Processing 8–14

Chapter 9 • Terminal Risk Management

9.1 Card Data 9–2
9.2 Terminal Data 9–3
9.3 GET DATA Command 9–4
9.4 Processing 9–4
9.4.1 Terminal Exception File 9–4
9.4.2 Merchant Forced Transaction Online 9–4
9.4.3 Floor Limits 9–4
9.4.4 Random Transaction Selection 9–4
9.4.5 Terminal Velocity Checking 9–5
9.4.6 New Card Check 9–5
9.5 Prior Related Processing 9–5
9.6 Subsequent Related Processing 9–6

Chapter 10 • Terminal Action Analysis

10.1 Card Data 10–2
10.2 Terminal Data 10–3
10.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command 10–4
10.4 Processing 10–4
10.4.1 Review Offline Processing Results 10–4
10.4.2 Request Cryptogram Processing 10–5
10.5 Prior Related Processing 10–5
10.6 Subsequent Related Processing 10–5

Chapter 11 • Card Action Analysis

11.1 Card Data 11–2
11.2 Terminal Data 11–5
11.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command 11–6
11.4 Processing 11–6
11.4.1 Card Receives Cryptogram Request 11–6
11.4.2 Card Risk Management 11–7
11.4.3 Card Risk Management Processes 11–9
11.4.3.1 Online Authorization Not Completed 11–9
11.4.3.2 Issuer Authentication Failed (or Mandatory and Not Performed) on Last Transaction 11–9
11.4.3.3 Static Data Authentication (SDA) Failed on Last Transaction 11–10
11.4.3.4 Dynamic Data Authentication (DDA) Failed on Last Transaction 11–10
11.4.3.5 Issuer Script Processed on Last Online Transaction 11–10
11.4.3.6 Velocity Checking for Total Consecutive Offline Transactions (Lower Limit) 11–10
11.4.3.7 Velocity Checking for Total Consecutive Offline International Transactions (Based on Currency) 11–11

11.4.3.8 Velocity Checking for Total Consecutive International Transactions (Based on Country) 11–11

11.4.3.9 Velocity Checking for Transaction Amount in Designated Currency 11–12

11.4.3.10 Velocity Checking for Transaction Amount (Dual Currency) 11–13

11.4.3.11 New Card 11–15

11.4.3.12 Offline PIN Verification Not Performed (PIN Try Limit Exceeded) 11–15

11.5 Card Provides Response Cryptogram 11–16

11.5.1 Card Declined Transaction Offline 11–17

11.5.2 Card Requested Online Processing 11–18

11.5.3 Card Approved Transaction Offline 11–18

11.5.4 Combined DDA/AC Generation Requested 11–19

11.6 Processing Flow 11–20

11.7 Prior Related Processing 11–26

11.8 Subsequent Related Processing 11–26

Chapter 12 • Online Processing

12.1 Card Data 12–2

12.2 Online Response Data 12–4

12.3 EXTERNAL AUTHENTICATE Command 12–5

12.4 Processing 12–5

12.4.1 Online Request 12–5

12.4.2 Online Response 12–5

12.4.3 Issuer Authentication 12–6

12.5 Processing Flow 12–8

12.6 Prior Related Processing 12–9

12.7 Subsequent Related Processing 12–9

Chapter 13 • Completion

13.1 Card Data 13–3

13.2 Terminal Data 13–6

13.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command 13–7

13.4 Completion Processing Overview 13–7

13.5 Receive GENERATE AC Command 13–9

13.6 Transaction Authorized Online 13–9

13.6.1 AAC (Decline) Requested After Online Authorization 13–10

13.6.2 TC (Approval) Requested After Online Authorization 13–11

13.6.2.1 Card Approves Transaction After TC (Approval) Requested 13–12

13.6.2.2 Card Declines Transaction After TC (Approval) Requested 13–13

13.7 Online Processing Requested, Online Authorization Not Completed 13–14

13.7.1 Card Risk Management 13–15

13.7.1.1 Velocity Checking for Total Consecutive Offline Transactions (Upper Limit) 13–15

13.7.1.2 New Card 13–15

13.7.1.3 PIN Try Limit Exceeded 13–16

13.7.1.4 Velocity Checking for Transaction Amount (Upper Limit) 13–16

13.7.1.5 Velocity Checking for Transaction Amount (Dual Currency) (Upper Limit) 13–16

13.7.2 Card Response After Unable to Go Online 13–17

13.7.2.1 Card Declined Transaction After Unable to Go Online 13–17

13.7.2.2 Card Approved Transaction After Unable to Go Online 13–18

13.8 Completion Processing Transaction Flow 13–20

13.9 Prior Related Processing 13–25

13.10 Subsequent Related Processing 13–25

Chapter 14 • Issuer-to-Card Script Processing

14.1 Key Management for Issuer Script Processing 14–3
14.2 Card Data 14–7
14.3 Terminal Data 14–8
14.4 Authorization Response Data 14–8
14.5 Commands 14–9
14.6 Processing 14–13
14.6.1 Authorization Response Message 14–13
14.6.2 Card Script Processing 14–13
14.6.3 Card Secure Messaging 14–14
14.6.4 Other Considerations 14–15
14.6.5 Resulting Indicators 14–15
14.6.6 Processing Flow 14–16
14.7 Prior Related Processing 14–17
14.8 Subsequent Related Processing 14–17

Chapter 15 • Personalization Considerations

15.1 VSDC Common Personalization 15–2
15.2 VSDC Flexible Approach 15–3

Appendix A • Card and Issuer Data Element Tables

A.1 Card and Issuer Data Element Descriptions A–2
A.2 Card and Issuer Data Element Requirements A–44
A.2.1 Tags A–44
A.2.2 Required Presence A–44
A.2.3 Data Integrity (Backup Required) A–44
A.2.4 Update Capability A–45
A.2.5 Retrieval Capability A–45
A.2.6 Static or Dynamic A–45

A.2.7 Secret Data A–45
A.2.8 ADF or DDF Data A–45
A.2.9 Data Requirements Chart A–46
A.2.10 Key to Data Requirements Chart A–58
A.3 Card and Issuer Data Element Tags A–60
A.4 Indicators and Counters A–65

Appendix B • Secure Messaging

B.1 Secure Messaging Format B–2
B.2 Message Integrity and Authentication (MACing) B–2
B.2.1 MAC Placement B–2
B.2.2 MAC Length B–2
B.2.3 MAC Key Generation B–2
B.2.4 MAC Computation B–2
B.3 Data Confidentiality B–5
B.3.1 Data Encipherment Key Calculation B–5
B.3.2 Enciphered Data Structure B–5
B.3.3 Data Encipherment Calculation B–5
B.3.4 Data Decipherment Calculation B–7
B.4 Session Key Generation B–8
B.5 Secure Messaging Impact on Command Formats B–9

Appendix C • Commands for Financial Transactions

C.1 Basic Processing Rules for Issuer Script Commands C–2
C.2 APPLICATION BLOCK Command—Response Application Protocol Data Units (APDUs) C–2
C.3 APPLICATION UNBLOCK Command—Response APDUs C–3
C.4 CARD BLOCK Command—Response APDUs C–3
C.5 EXTERNAL AUTHENTICATE Command—Response APDUs C–3

C.6 GENERATE APPLICATION CRYPTOGRAM (AC) Command—Response APDUs C–4
C.7 GET CHALLENGE Command—Response APDUs C–5
C.8 GET DATA Command—Response APDUs C–5
C.8.1 Command Support C–5
C.8.2 Data Retrievable by GET DATA Command C–6
C.8.2.1 Special Devices C–6
C.8.2.2 Financial Transactions C–7
C.9 GET PROCESSING OPTIONS Command—Response APDUs C–8
C.10 INTERNAL AUTHENTICATE Command—Response APDUs C–8
C.11 PIN CHANGE/UNBLOCK Command—Response APDUs C–8
C.11.1 PIN Data Generated Using the Current PIN C–9
C.11.2 PIN Data Generated Without Using the Current PIN C–10
C.12 PUT DATA Command—Response APDUs C–11
C.12.1 Command Message C–12
C.12.2 Processing State Returned in the Response Message C–13
C.13 READ RECORD Command—Response APDUs C–14
C.14 SELECT Command-Response APDUs C–14
C.15 UPDATE RECORD Command—Response APDUs C–16
C.15.1 Command Message C–16
C.15.2 Processing State Returned in the Response Message C–17
C.16 VERIFY Command—Response APDUs C–18

Appendix D • Authentication Keys and Algorithms

D.1 Source Data D–2
D.2 Generating the TC, AAC, and ARQC D–4
D.3 Generating the Authorization Response Cryptogram (ARPC) D–6

D.4 Data Conversion D–8
D.4.1 All Data D–8
D.4.2 Numeric Data D–8
D.4.3 Compressed Numeric Data D–9
D.4.4 Binary Data D–9
D.4.5 Alphanumeric and Alphanumeric Special Data D–9
D.5 Derivation Key Methodology D–10
D.6 Host Security Modules (HSM) D–13
D.6.1 Real-Time Host-Based Cryptographic Functions D–13
D.6.2 Personalization Support Cryptographic Functions D–14

Appendix E • Cryptogram Versions Supported

E.1 Cryptogram Version 10 . . . . . E–2
E.2 Cryptogram Version 12 . . . . . E–3
E.3 Cryptogram Version 14 . . . . . E–3

Appendix F • Card Internal Security Architecture

F.1 Objective of ICC Internal Security F–1
F.2 Overview of ICC Internal Security F–1
F.2.1 Security Domain F–2
F.2.2 Elementary File Access Conditions F–3
F.3 File Control Information F–3
F.3.1 Application Management Data F–3
F.3.1.1 Security Domain F–3
F.3.2 Data Resources F–4
F.3.2.1 Data Identification F–4
F.3.2.2 Key Identification F–5
F.3.2.3 PIN/Password Identification F–5

F.3.3 Executable Code Resource F–5
F.3.3.1 Command Identification F–5
F.3.3.2 Algorithm Identification F–5
F.4 File Control Parameters F–6
F.5 ICC Card Resident Data Recommended Access Conditions F–7

Appendix G • Card Requirements for Visa Low-Value Payment Feature

G.1 Card Data G–2
G.2 Terminal Data G–4
G.3 VLP Purchase Transaction Process G–5
G.3.1 Application Selection G–5
G.3.2 Initiate Application Processing G–5
G.3.3 Card Action Analysis G–6
G.3.4 Online Processing G–6
G.3.5 Completion G–6
G.4 VLP Reset Transaction Processing G–7
G.5 Updating the VLP Limits G–7
G.6 VLP Transaction Flow G–8

Appendix H • Acronyms

Glossary

Index

Figures

2–1: Sample Transaction Flow 2–7
3–1: Sample Card Directory Structure 3–9
3–2: Application Selection Using Directory Method 3–12
3–3: Application Selection Using List of AIDs 3–13
4–1: Initiate Application Processing Flow 4–6
8–1: Checking The PIN Try Counter 8–10
8–2: PIN Encipherment 8–10
8–3: Offline PIN Processing 8–13
11–1: Card Action Analysis Processing Flow (1 of 6) 11–20
11–2: Card Action Analysis Processing Flow (2 of 6) 11–21
11–3: Card Action Analysis Processing Flow (3 of 6) 11–22
11–4: Card Action Analysis Processing Flow (4 of 6) 11–23
11–5: Card Action Analysis Processing Flow (5 of 6) 11–24
11–6: Card Action Analysis Processing Flow (6 of 6) 11–25
12–1: Online Processing Flow 12–8
13–1: Completion Processing Flow 13–8
13–2: Transaction Flow (1 of 5) 13–20
13–3: Transaction Flow (2 of 5) 13–21
13–4: Transaction Flow (3 of 5) 13–22
13–5: Transaction Flow (4 of 5) 13–23
13–6: Transaction Flow (5 of 5) 13–24
14–1: Generation and Use of MAC Keys 14–4
14–2: Generation and Use of Data Encipherment Keys 14–6
14–3: Issuer-to-Card Script Processing Flow 14–16
15–1: Personalization Overview 15–1

B–1: MAC Algorithm for Double-Length DEA Key B–4

B–2: Data Encipherment for Double-Length DEA Key B–6

B–3: Data Decipherment for Double-Length DEA Key B–7

D–1: Algorithm for Generating the TC/AAC or ARQC D–5

D–2: Algorithm for Generating the ARPC D–7

D–3: Derivation Method of Unique DEA Keys A and B D–10

D–4: Using the Unique DEA Keys to Perform Card Authentication D–12

G–1: VLP Transaction Flow (1 of 2) G–8

G–2: VLP Transaction Flow (2 of 2) G–9

Tables

2–1: Card Functional Requirements 2–8
2–2: Command Support Requirements 2–10
3–1: Application Selection—Card Data 3–2
3–2: Application Selection—Terminal Data 3–5
3–3: Sample Matching AIDs 3–10
4–1: Initiate Application Processing—Card Data 4–2
4–2: Initiate Application Processing—Terminal Data 4–3
5–1: Read Application Data—Card Data 5–2
5–2: Read Application Data—Card Files 5–2
6–1: Offline Data Authentication—Card Data 6–6
6–2: Card Data Used in SDA 6–7
6–3: Offline Data Authentication—SDA Related Card Data 6–9
6–4: Offline Data Authentication—DDA Card Data 6–11
6–5: Offline Data Authentication—Internal Card Data Used During DDA 6–12
6–6: Offline Data Authentication—DDA Terminal Data 6–13
7–1: Processing Restrictions—Card Data 7–2
7–2: Processing Restrictions—Terminal Data 7–3
7–3: Application Usage Control (AUC) 7–5
8–1: CVM List Processing—Card Data 8–2
8–2: Sample CVM List 8–5
8–3: Offline PIN Processing—Card Data 8–6
8–4: Offline Enciphered PIN Processing—Card Data 8–7
8–5: PIN Processing—Terminal Data 8–8
9–1: Terminal Risk Management—Card Data 9–2
9–2: Terminal Risk Management—Terminal Data 9–3

10–1: Terminal Action Analysis—Card Data 10–2
10–2: Request Cryptogram Processing—Card Data 10–3
10–3: Review Offline Processing Results—Terminal Data 10–3
10–4: Request Cryptogram Processing—Terminal Data 10–4
11–1: Card Action Analysis—Card Data 11–2
11–2: Card Action Analysis—Terminal Data 11–5
11–3: Card Risk Management Checks 11–7
11–4: Card's Response to First GENERATE AC Command 11–16
12–1: GENERATE AC Response—Card Data 12–2
12–2: Issuer Authentication Decision—Card Data 12–3
12–3: Online Processing, Issuer Authentication—Card Data 12–3
12–4: Online Processing—Terminal Data 12–4
13–1: Completion—Card Data 13–3
13–2: GENERATE AC Command Response 13–5
13–3: Completion—Card Data Used by Terminal 13–6
13–4: Completion—Terminal Data 13–6
14–1: Issuer-to-Card Script Processing—Card Data 14–7
14–2: Issuer-to-Card Script Processing—Terminal Data 14–8
14–3: Issuer-to-Card Script Processing—Online Response Data 14–8
15–1: Sample Flexible Card Functionality 15–3
A–1: Card and Issuer Data Element Descriptions A–3
A–2: Data Requirements A–46
A–3: Data Requirements Chart Key A–58
A–4: Card Data Element Tags A–60
A–5: Setting of Indicators and Counters A–65
C–1: Static Data Retrieval Using GET DATA C–6
C–2: Data Retrieval Using GET PROCESSING OPTIONS C–8
C–3: Data to be Updated With PUT DATA C–11
C–4: PUT DATA Command Message C–12
C–5: PUT DATA Command Message Warning Conditions C–13
C–6: PUT DATA Command Message Error Conditions C–13
C–7: UPDATE RECORD Command Message C–16
C–8: UPDATE RECORD Reference Control Parameter C–16

C–9: UPDATE RECORD Message Warning Conditions C–17
C–10: UPDATE RECORD Message Error Conditions C–17
D–1: TC/AAC/ARQC Data Elements Order D–3
E–1: Creating a TC/AAC and ARQC With Cryptogram Version 10 . . . . . E–2
F–1: Available Access Conditions for an Elementary File F–6
G–1: Initiate Application Processing—Card Data G–2
G–2: Duplicate Data Elements for VLP G–3
G–3: Initiate Application Processing—Card Data G–4
G–4: Initiate Application Processing—Terminal Data G–4
H–1: Acronyms H–1

About This Specification 1

The *Visa Integrated Circuit Card Specification* (VIS) provides the technical details of chip card and terminal functionality related to Visa Smart Debit and Visa Smart Credit (VSDC) transactions (Visa's chip-based credit and debit programs). It focuses on the functions performed by the chip card and terminal as well as the interaction between the chip card and terminal at the point of transaction.

The objective of the *Visa Integrated Circuit Card Specification* is to:

- Communicate the implementation details of Europay, MasterCard, and Visa (EMV) specifications to ease vendor development efforts
- Aid members and vendors in understanding the changes that chip brings to the credit and debit payment services, especially in terms of the processing taking place between the chip card and terminal at the point of transaction
- Provide Visa's minimum requirements for chip-based credit and debit programs
- Identify options that members and vendors can implement to meet market needs
- Support Visa's payment service rules and International Operating Regulations for Visa Smart Debit and Visa Smart Credit (VSDC)
- Define Visa's implementation of optional EMV features

Because VIS is based on EMV, the two specifications should be used together for reference and development purposes. However, VIS builds on the EMV requirements in order to support the Visa payment service rules. To facilitate understanding of the differences between these two specifications, please refer to Chapter 2, Processing Overview.

1.1 Audience

This document is intended for members, vendors, and readers seeking a technical understanding of the functionality of chip cards and terminals supporting Visa Smart Debit and Visa Smart Credit programs.

1.2 VIS Update

This document serves as an update to VIS 1.3.2. The update includes changes reflecting EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, enhancements to VSDC functionality, and corrections and clarifications to VIS 1.3.2. An impacts summary highlighting the differences between VIS 1.3.2 and the current version, VIS 1.4.0, is provided later in this chapter.

1.3 Terminology

This section provides clarification on several terms used throughout the specification.

1.3.1 Mandatory/Required/Recommended/Optional

Visa's philosophy is to facilitate market requirements while ensuring global interoperability. To this end, Visa's minimum requirements reflect the EMV mandatory items in addition to specific requirements outlined in the Visa payment service rules or International Operating Regulations. All other functionality is optional and not required.

Visa's minimum requirements are designated using the terms "mandatory", "required", and "shall". Recommended functionality is highlighted in the document and designated using the term "should". Elective data elements and functions are designated using the terms "optional" or "may."

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

1.3.2 Card/Integrated Circuit

In general, the term "card" is used to describe functions performed by the VSDC application on the card. When it is necessary to distinguish between the chip itself and another card feature such as the magnetic stripe, the term "integrated circuit" may be used.

1.3.3 Terminated Transactions

When the term "terminal terminates transaction" is used, it includes the processing to end the transaction and the display of the message to the cardholder and merchant indicating why the transaction cannot be completed.

1.4 Document Structure

This section provides an overview of the structure of the *Visa Integrated Circuit Card Specification*. It begins with an overview of the three volumes, is followed by an overview of each chapter, and concludes with the sub-heading structure of each chapter.

1.4.1 Volume Overview

The document is organized into three volumes:

- **Application Volume**—This volume provides a technical overview of the processing between the card and terminal. This volume may be used as an overview to understand the processing and sequence of events involved in a VSDC transaction flow.
- **Card Volume**—This volume specifies the technical details of EMV related to the data and processing performed by the card. It also includes additional Visa specific requirements for card functionality. Vendors involved in the creation of the VSDC card application should focus on this document for their development efforts.
- **Terminal Volume**—This volume specifies the technical details of EMV related to the data and processing performed by the terminal. It also includes additional Visa specific requirements for terminal functionality. Vendors involved in the creation of the VSDC terminal application should focus on this document for their development efforts.

To provide clarity, requirements from EMV may be restated in the various volumes and, where necessary, information is replicated in the three volumes to provide comprehensive information. Each volume includes a list of acronyms, a glossary, and an index.

1.4.2 Chapter Overview

This guide is organized according to the functions that occur during VSDC transaction flow and is divided into the following sections:

Chapter 1, About This Specification—This chapter provides an overview of the VIS specification, VIS terminology, a summary of revisions for this version of the VIS documents, and a list of reference materials.

Chapter 2, Processing Overview—This chapter provides an overview of the each function and highlights whether the function is mandatory or optional.

Chapter 3, Application Selection—This function determines which of the applications, supported by both the card and terminal, will be used to conduct the transaction.

Chapter 4, Initiate Application Processing—During this function, the card receives any terminal data which was requested by the card during Application Selection.

Chapter 5, Read Application Data—During this function, the terminal reads the data records necessary for the transaction from the card.

Chapter 6, Offline Data Authentication—During this function, the terminal authenticates data from the card using RSA public key technology.

Chapter 7, Processing Restrictions—During this function, application version checks, effective and expiration dates checks, and other checks are performed by the terminal at the point of transaction.

Chapter 8, Cardholder Verification—During this function, the terminal determines the cardholder verification method (CVM) to be used and performs the selected CVM.

Chapter 9, Terminal Risk Management—During this function, the terminal ensures that higher-value transactions are sent online and that chip-read transactions go online periodically. This risk management check protects against threats that might be undetectable in an offline environment.

Chapter 10, Terminal Action Analysis—During this function, the terminal applies rules set by the issuer in the card and by the acquirer in the terminal to the results of offline processing. This analysis determines whether the transaction should be approved offline, declined offline, or sent online for an authorization.

Chapter 11, Card Action Analysis—During this function, velocity checking and other risk management, internal to the card, is performed.

Chapter 12, Online Processing—During this function, the issuer's host computer reviews and authorizes or rejects transactions using the issuer's host-based risk parameters.

Chapter 13, Completion—During this function, the card and the terminal conclude transaction processing.

Chapter 14, Issuer-to-Card Script Processing—During this function, the card applies post-issuance changes sent from the issuer.

Chapter 15, Personalization Considerations

Appendix A, Data Elements—This appendix defines the data elements used in processing the VSDC application from a card and issuer perspective.

Appendix B, Secure Messaging—This appendix provides the technical details for secure messaging related to issuer-to-card script processing.

Appendix C, Commands for Financial Transactions—This appendix outlines the commands used during transaction processing.

Appendix D, Authentication Keys and Algorithms—This appendix describes the keys and algorithms associated with the generation of the online authentication cryptograms (ARQC, TC, AAC).

Appendix E, Cryptogram Versions Supported—This appendix provides the methods and data elements used to generate the online authentication cryptograms (ARQC, TC, AAC).

Appendix F, Card Internal Security Architecture—This appendix describes the chip card's internal security framework. This framework is used by the card operating system to ensure that appropriate security mechanism are used to provide security and integrity for all data and processes by the card.

Appendix G, Visa Low-Value Payment—This appendix describes card processing for the optional VLP feature used for rapid processing of low value payments.

1.4.3 Subheading Overview

For ease of use, the main chapters are structured in the same manner:

- **Card Data**—Provides the mandatory and optional data elements required on the card to support the function. Data element tags are listed when multiple tags are associated with a single data element name.
- **Terminal Data**—Provides the mandatory and optional data elements needed in the terminal to support the function. Data element tags are listed when multiple tags are associated with a single data element name.
- **Commands**—Provides the requirements for the commands used to support the function.
- **Processing**—Provides the technical details of the function. If there are several functions within a process, they may be listed separately.

  NOTE: *Flowcharts are representative of processing and may not include all steps that may be performed.*

- **Prior Related Processing**—Outlines prior processing to aid in understanding previous activities related to this function.
- **Subsequent Related Processing**—Outlines subsequent processing to aid in understanding future activities related to this function.

1.5 Revisions to This Specification

Revisions to this specification may be required to accommodate future EMV changes, Visa payment service rules, or market needs. The impacts of these changes will be communicated in the VIS changes list or in an update to this document.

1.6 Impact Summary

The following sections are an outline of changes and additional functionality from both a terminal and card perspective for VIS 1.4.0 (April 2001).

1.6.1 Terminal

This section includes mandatory and optional changes. The testing of terminals to support mandatory changes shall be aligned with the EMV 2000, Version 4.0, migration requirements. Refer to the EMVCo website for information on testing schedules.

1.6.1.1 Mandatory

- If the Directory method of Application Selection fails, the terminal shall switch to the List of AIDs method.
- The terminal shall not allow Partial Selection during Application Selection if the terminal indicators show it is not supported for the AID.
- During SDA and DDA, the terminal shall save the Data Authentication Code (if present) and ICC Dynamic Number after recovery.
- If the SDA Tag List is one of the data elements read from the card, the terminal shall validate that the only tag it contains is the tag for the AIP.
- ATMs supporting Offline PIN shall support CVM List processing.

1.6.1.2 Optional

This section includes mandatory and optional changes. Contact the CAA for information on testing schedules. Changes are backward compatible and cards tested under versions 1.3.1 and 1.3.2 will continue to work in the new devices.

- Visa Operating Regulations may permit the terminal to eliminate certain common applications from consideration during Application Selection.
- The EMV Combined DDA/Generate AC option is included as a terminal option.
- The public key encipherment used in the Offline Enciphered PIN processing may occur either in the PIN pad or in the card reader. Secure transfer of the PIN from the PIN pad to the card reader is required.
- Terminal support for Visa Low-value Payment feature of VSDC.

1.6.2 Card

This section includes mandatory and optional changes. Contact the CAA for information on testing schedules. Changes are backward compatible and cards tested under versions 1.3.1 and 1.3.2 will continue to work in the new devices.

1.6.2.1 Mandatory

- If a card is personalized with an SDA Tag List, the only tag in the list must be “82”, the tag for the Application Interchange Profile. Prior to adding this requirement to EMV a survey was conducted to determine if the SDA tag list was being utilized. The results indicated that it was not in use and that the requirement could be added to EMV. To ensure interoperability and backward compatibility cards should begin compliance immediately. An SDA tag list that does not comply will result in Offline Data Authentication failure in EMV 4.0 terminals.
- Support of Cardholder Verification must be indicated in the Application Interchange Profile and a CVM List is required.
- Cumulative amounts are no longer incremented for offline declines.
- The Online Authorization Indicator is no longer reset after offline approval.

1.6.2.2 Optional

- The Issuer Public Key length may equal that of the corresponding Visa CA Public Key.
- The ICC Public Key length may equal that of the corresponding Issuer Public Key.
- The EMV Combined DDA/Generate AC option is included as a VSDC card option.
- The EMV optional session key generation method is referenced as a VIS option.
- A new cryptogram generation method, Cryptogram Version 14, is referenced as a VIS option.

  NOTE: *Cryptogram Version 14 is not currently supported in VisaNet systems and Issuers wishing to implement this option must be aware that they will not be eligible for VisaNet Authentication Services.*

- The Online Authorization Indicator is optional in the card unless Issuer Authentication or Issuer Script processing is supported.
- The Visa Low-value Payment feature of VSDC has been added.
- A “Cumulative Total Transaction Amount Upper Limit” has been added.
- An Application Default Action bit has been added to allow issuers to send transactions online if issuer script processing failed on a previous transaction.
- An Application Default Action bit has been added to allow issuers to decline the transaction and block the application if the PIN Try Limit was exceeded on a previous transaction.

1.7 Reference Materials

The following documents contain additional information on Visa Smart Debit and Visa Smart Credit. The websites for obtaining these documents or information on obtaining them are listed below. For additional information, contact your Visa member representative.

1.7.1 International Organisation for Standardisation (ISO) Documents

Information on ordering these documents is available on http://www.iso.ch

- *ISO 639:1988. Codes for the Representation of Names and Languages.*
- *ISO 3166:1997. Codes for the Representation of Names of Countries.*
- *ISO 4217:1995. Codes for the Representation of Currencies and Funds.*
- *ISO/IEC 7810:1995. Identification Cards—Physical Characteristics.*
- *ISO/IEC 7811:1995. Identification Cards—Recording Technique.*
- *ISO/IEC 7812:1994. Identification Cards—Identification of Issuers.*
- *ISO/IEC 7813:1995. Identification Cards—Financial Transaction Cards*
- *ISO/IEC 7816-4:1995. Identification Cards—Integrated Circuit Cards with Contacts—Part 4: Interindustry Commands for Interchange.*
- *ISO/IEC 7816-5:1994. Identification Cards—Integrated Circuit Cards with Contacts—Part 5: Numbering System and Registration Procedure for Application Identifiers.*
- *ISO 8583:1987. Bank Card Originated Messages—Interchange Message Specifications—Content for Financial Transactions.*
- *ISO 8583:1993. Financial Transaction Card Originated Messages—Interchange Message Specifications.*
- *ISO 8859:1987. Information Processing—8-bit Single-Byte Coded Graphic Character Sets.*
- *ISO 9564:1991. Banking—Personal Identification Number Management and Security.*

1.7.2 EMV Documents

Available on the EMVCo Website:
http://www.emvco.com/specifications.cfm

- *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, Book 1, Application Independent ICC to Terminal Interface Requirements*, December, 2000.
- *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, Book 2, Security and Key Management*, December, 2000.
- *EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Version 4.0, Book 3, Application Specification*, December, 2000.
- *EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Version 4.0, Book 4, Cardholder, Attendant and Acquirer Interface Requirements*, December, 2000.

1.7.3 Visa Documents

Available on the Visa website:
http://wwws2.visa.com/nt/chip/visdownload.html

- *Visa Integrated Card Specification* (Application Overview, Card Specification, and Terminal Specification) (VIS - versions 1.3.2 and 1.4.0)
- VIS Corrections and Updates

Available on the Visa website:
http://visa.com/nt/suppliers/vendor

- *Chip Card Products: Submission Requirements*—Describes Visa International requirements for approval of new and upgraded chip card products.

  Visa supports and recognizes approvals by EMVCo, LLC for EMV level 1 (Interface Module) and EMV level 2 (device application). EMVCo is the owner of the EMV Integrated Circuit Card Specifications for Payment Systems.

  EMVCo specifications, type approval administrative documentation, test requirements and test cases for EMV levels 1 and 2 may be obtained through the EMVCo website www.emvco.com.

- *Chip Card Products: Testing and Approval Requirements*—Describes Visa International requirements for approval of new and upgraded chip card products. It summarized Visa's present testing services, policies, and pricing.

- *Common Personalization*—A guide to a common approach to personalization of all applications.

  NOTE: *This guide is the final authority for non-application specific requirements.*

Available on Visa InSite Global Products eLibrary: (http://insite/global/Consumer Platform Search/content) or through a regional representative:

- *Certificate Authority User's Guide—Visa Smart Debit and Visa Smart Credit, Visa Cash*—Information and procedures related to the Visa Certificate Authority including Visa Certificate Authority Public Keys and Issuer Public Key Certificates.
- *Common Personalization for Visa Smart Debit and Credit (VSDC)*—A guide to personalization of VSDC Applications using the Common Personalization Approach.

  NOTE: *The Visa Smart Debit and Visa Smart Credit Personalization Templates have been added to this document.*
- *Visa Smart Debit and Visa Smart Credit Certification Authority Key Revocation Visa Policies and Procedures*—The Visa-specific policies and procedures related to key revocation.
- *Visa Smart Debit and Visa Smart Credit Member Implementation Guide for Acquirers*—Describes best practices, suggestions, considerations, and step-by-step activities to assist with implementation for VSDC Acquirers.
- *Visa Smart Debit and Visa Smart Credit Member Implementation Guide for Issuers*—Describes best practices, suggestions, considerations, and step-by-step activities to assist with implementation for VSDC Acquirers.
- *Visa Smart Debit and Visa Smart Credit Planning Guide*—A reference guide and roadmap for Acquirers and Issuers implementing Visa Smart Debit or Visa Smart Credit programs. It describes the components and decisions necessary for program implementation and focuses on what is new and different about implementing a Visa Smart Debit or Visa Smart Credit program.
- *VSDC Service Activation Guide (SAG)*—Describes planning considerations, business aspects, technical aspects and other regional tasks associated with completing a member implementation of VSCD.
- *Visa Smart Debit/Visa Smart Credit Service Description*—A document focusing on the features and benefits of the service.

Available on Visa InSite or through a Visa regional representative: http://insite/ref/docs

- *Card Acceptance Device Reference Guide: Requirements and Best Practices Version 5.0*—Provides vendors with insight towards designing their card acceptance devices to meet current and future industry and Visa scheme specific requirements and best practices.
- *Visa Certification Management Service (VCMS) Testing and Certification Guide-VIP System, Member Version*—A guide for the VIP System component of the VisaNet Certification Management System.
- *Visa Certification Management Service (VCMS) User's Manual-BASE II System*—A guide for the BASE II System component of the VisaNet Certification Management System.
- *VisaNet Card Technology Standards Manual*—The standards applied to PINs, PIN-related security, and the management of cryptographic keys as well as the guidelines for encoding account and cardholder data on Track 1 and Track 2 of the magnetic stripe of a Visa card.

Available on Visa InSite or through a Visa regional representative: http://insite/dept/buspubs1/library/vsmart/techlet.pdf

- *Visa Smart Debit and Visa Smart Credit System Technical Manual*—A document that describes the changes to VisaNet to support VSDC.

Available on Visa InSite or through a Visa regional representative: http://insite/dynaweb/opregs

- *Visa International Operating Regulations*—Specifies standards all Members must meet to operate and participate in Visa Payment Services (Volumes I-IV).

Available through Visa regional representative:

- *Visa Smart Debit/Credit Certificate Authority Internal Procedures*—Describes guidelines for enrolling the Visa Certificate Authority and is intended for use by Regional staff supporting VSDC.
- *Visa Smart Payment Operating Principles Guide*—Board-approved payment service principles for Visa Smart Debit and Visa Smart Credit.

Available by request to the VSDC Hotline:

- *Visa Smart Debit/Visa Smart Credit Early & Full Data Options for Host Systems*—Provide Member center managers with an overview of the Early and Full options for their host systems.

Processing Overview 2

This chapter provides an overview of a Visa Smart Debit and Visa Smart Credit (VSDC) transaction. This is followed by a transaction flow showing the order in which these functions may be performed and the commands sent by the terminal to the card for communications. Charts at the end of the chapter show functional and command support requirements for cards and terminals.

Regions may have additional restrictions and requirements.

2.1 Functional Overview

The following functions are used in VSDC transaction processing. Functions marked as *mandatory* are performed for all transactions. Some steps within these mandatory functions may be optional. Functions not marked *mandatory* are optional and are performed based upon parameters in the card or terminal, or both.

2.1.1 Application Selection (mandatory)

When a VSDC card is presented to a terminal, the terminal determines which applications are supported by both the card and terminal. The terminal displays all mutually supported applications to the cardholder, and the cardholder selects the application to be used for payment. If these applications cannot be displayed, the terminal selects the highest priority application as designated by the issuer during card personalization.

2.1.2 Initiate Application Processing/Read Application Data (mandatory)

If a VSDC application is selected, the terminal requests that the card indicate the data to be used for that application and the functions supported. The card may indicate different data or different support functions based upon characteristics of the transaction such as being domestic or international. The terminal reads the data indicated by the card and uses the supported function list to determine the processing to perform.

2.1.3 Offline Data Authentication

The terminal determines whether it should authenticate the card offline using either offline static or dynamic data authentication based upon the card and terminal support for these methods.

Offline Static Data Authentication (SDA) validates that important application data has not been fraudulently altered since card personalization. The terminal validates static (unchanging) data from the card using the card's Issuer Public Key, which is stored on the card inside a public key certificate and a digital signature, which contains a hash of important application data encrypted with the Issuer Private Key. A match of the recovered hash with a generated hash of the actual application data proves that the data has not been altered.

Offline Dynamic Data Authentication (DDA) validates that the card data has not been fraudulently altered and that the card is genuine. DDA has two forms: Standard DDA and Combined DDA/Generate AC. In both forms, the terminal verifies the card static data in a similar manner to SDA.

With Standard DDA, the terminal requests that the card generate a cryptogram using dynamic (transaction unique) data from the card and terminal and an ICC Private Key. The terminal decrypts this dynamic signature using the ICC Public Key recovered from card data. A match of the recovered data to the original data verifies that the card is not a counterfeit card created with data skimmed (copied) from a legitimate card.

With Combined DDA/Generate AC, the generation of the dynamic signature is combined with the generation of the card's Application Cryptogram during Card Action Analysis to assure that the Application Cryptogram came from the valid card.

2.1.4 Processing Restrictions (mandatory)

The terminal performs Processing Restrictions to see whether the transaction should be allowed. The terminal checks whether the effective date for the card has been reached, whether the card is expired, whether the application versions of the card and terminal match, and whether any Application Usage Control restrictions are in effect. An issuer may use Application Usage Controls to restrict a card's use for domestic or international, cash, goods, services, or cashback.

2.1.5 Cardholder Verification (mandatory)

Cardholder verification may be used to ensure that the cardholder is legitimate and the card is not lost or stolen. The terminal uses a Card Verification Method (CVM) List from the card to determine the type of verification to be performed. The CVM List establishes a priority of cardholder verification methods, which consider the capabilities of the terminal and characteristics of the transaction to prompt the cardholder for a specific cardholder verification method. If the CVM is offline PIN, the terminal prompts the cardholder for a PIN and transmits the cardholder-entered PIN to the card, which compares it to a Reference PIN stored secretly in the card. The CVM List may also specify online PIN, signature, or no cardholder verification required.

The terminal may use a default CVM as defined by Visa International Operating Regulations if the card does not support CVM processing, no CVM list is present or the last CVM processed in the card list is No CVM Required.

2.1.6 Terminal Risk Management (mandatory)

Terminal Risk Management checks whether the transaction is over the merchant floor limit, the account number is on an optional terminal exception file, the limit for consecutive offline transactions has been exceeded, the card is a new card, or the merchant has forced the transaction online. Some transactions are randomly selected for online processing.

Terminal Risk Management also includes optional velocity checking by the terminal using data elements from the card. The card data elements used are those defined by Europay, MasterCard, and Visa (EMV) specifications. Terminal velocity checking results are considered during Terminal Action Analysis.

Visa recommends support for velocity checking by the card and the data elements used card velocity checks are defined by Visa. Card velocity checking results are considered during Card Action Analysis.

2.1.7 Terminal Action Analysis (mandatory)

Terminal Action Analysis uses the results of Offline Data Authentication, Processing Restrictions, Terminal Risk Management, and Cardholder Verification and rules set in the card and terminal to determine whether the transaction should be approved offline, sent online for authorization, or declined offline. The card rules are set in fields called Issuer Action Codes (IACs) sent to the terminal by the card. The payment system rules are set in Terminal Action Codes (TACs). After determining the transaction disposition, the terminal requests an application cryptogram from the card. The type of application cryptogram is based upon the transaction disposition with a Transaction Certificate (TC) for an approval, an Authorization Request Cryptogram (ARQC) for online, and an Application Authentication Cryptogram (AAC) for a decline. The terminal's request indicates whether the transaction is eligible for Combined DDA/AC Generation.

2.1.8 Card Action Analysis (mandatory)

Upon receiving the application cryptogram request from the terminal, the card performs Card Action Analysis where Card Risk Management checks may be performed to determine whether to change the transaction disposition set by the terminal. These may include checks for prior incomplete online transactions, failure of Issuer Authentication or offline data authentication failure on a previous transaction, and count or amount velocity checking limits being reached. The card may convert a terminal request for an offline approval to an online transaction or an offline decline. The card cannot override a terminal decision to decline a transaction.

After completion of the checks, the card generates the application cryptogram using application data and a secret DES key stored on the card. It returns this cryptogram to the terminal. For offline approved transactions, the TC and the data used to generate it are transmitted in the clearing message for future cardholder disputes, or chargeback purposes, or both. The TC may be used as a "proof" of transaction when a cardholder disputes a transaction and to verify that the transaction data has not been changed by the merchant or acquirer. For offline declined transactions, the cryptogram type is an AAC. For transactions to be authorized online, the cryptogram type is an ARQC.

2.1.9 Online Processing

If the card and terminal determine that the transaction requires an online authorization, the terminal transmits an online authorization message to the issuer if the terminal has online capability. This message includes the ARQC cryptogram, the data used to generate the ARQC, and indicators showing offline processing results. During online processing, the issuer validates the ARQC to authenticate the card in a process called Online Card Authentication (CAM). The issuer may consider these CAM results and the offline processing results in its authorization decision.

The authorization response message transmitted back to the terminal may include an issuer-generated Authorization Response Cryptogram (ARPC) (generated from the ARQC, the Authorization Response Code, and the card's secret DES key). The response may also include post-issuance updates to the card called Issuer Scripts.

If the authorization response contains an ARPC and the card supports Issuer Authentication, the card performs Issuer Authentication by validating the ARPC to verify that the response came from the genuine issuer (or its agent). Successful Issuer Authentication may be required for resetting certain security-related parameters in the card. This prevents criminals from circumventing the card's security features by simulating online processing and fraudulently approving a transaction to reset counters and indicators. If Issuer Authentication fails, subsequent transactions for the card will be sent online for authorization until Issuer Authentication is successful. The Issuer has the option to set up the card to decline the transaction if Issuer Authentication fails.

2.1.10 Issuer-to-Card Script Processing

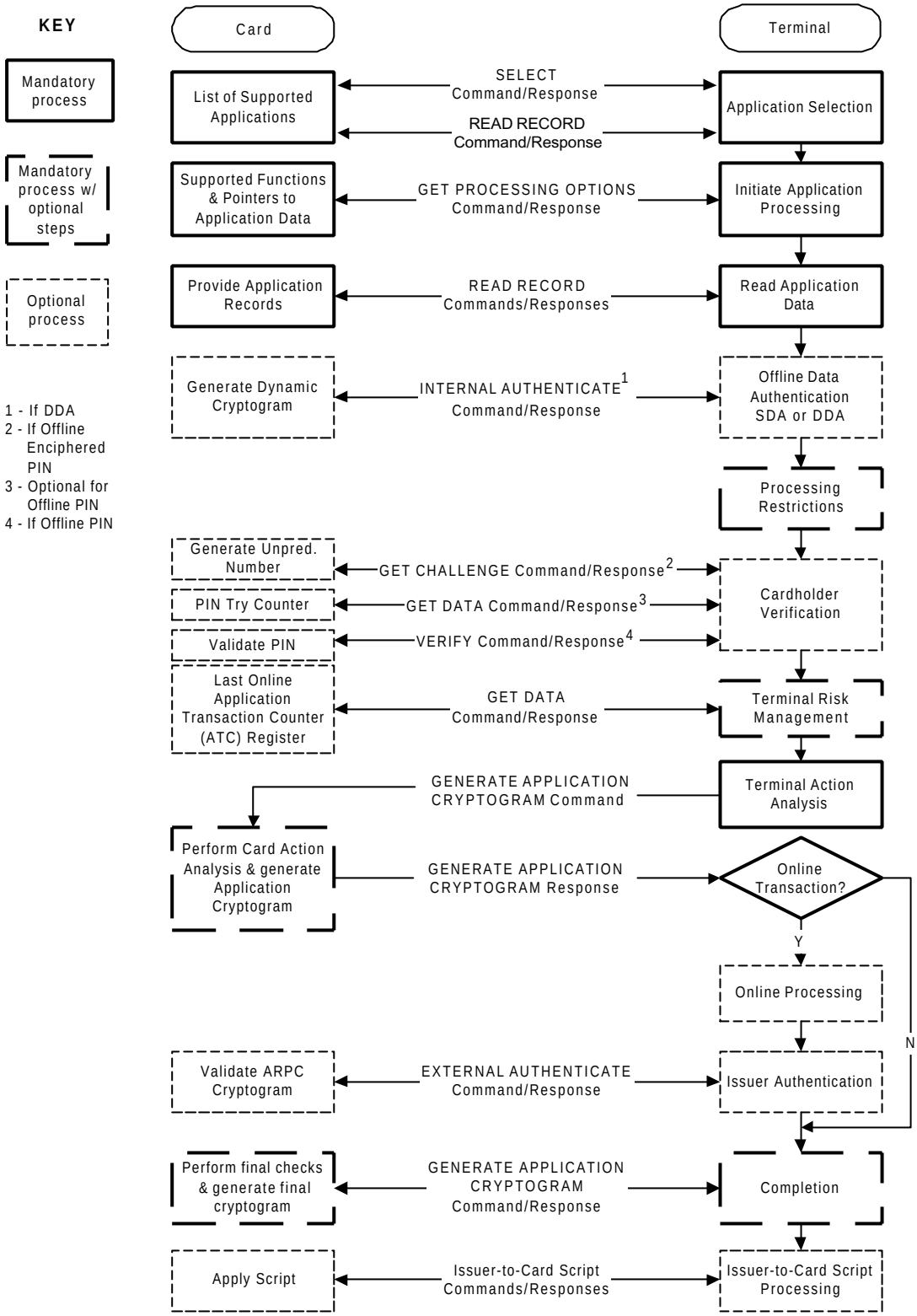
If the issuer includes script updates in the authorization response message, the terminal passes the script commands to the card. Prior to applying the updates, the card performs security checking to assure that the script came from the valid issuer and was not altered in transit. Supported script commands allow updating offline processing parameters, blocking and unblocking the application, blocking the card, resetting the Offline PIN Try Counter, and changing the Offline PIN value.

2.1.11 Completion (mandatory)

The card and terminal perform final processing to complete the transaction. An issuer-approved transaction may be converted to a decline based upon Issuer Authentication results and issuer-encoded parameters in the card. The card uses the transaction disposition, Issuer Authentication results, and issuer-encoded rules to determine whether to reset card-based counters and indicators. The card generates a TC for approved transactions and an AAC for declined transactions.

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 must generate a reversal for issuer-approved transactions which are subsequently declined by the card.

Figure 2–1: Sample Transaction Flow



2.2 Mandatory and Optional Functionality

2.2.1 Card Functional Requirements

VSDC cards must support the mandatory functions listed in Table 2–1. Optional functions may be supported at the issuer's discretion or may be required by market, regional, or Visa rules. Support for conditional functions is required if the associated condition is true.

Table 2–1: Card Functional Requirements (1 of 2)

Function	Card Support
Application Selection	Mandatory
• Directory Method	Optional (EMV)
• Explicit Selection Method	Mandatory (EMV)
Initiate Application Processing	Mandatory (EMV)
Read Application Data	Mandatory (EMV)
Offline Data Authentication	Optional (EMV)
• SDA	Optional (EMV) Conditional—If DDA supported (VIS)
• Standard DDA	Optional (EMV) Conditional—If Combined DDA/AC Generation supported (VIS)
• Combined DDA/AC Generation	Optional (EMV)
Processing Restrictions	Mandatory (EMV)
• Application Version Number	Mandatory (EMV)
• Application Usage Control	Optional (EMV)
• Effective Date Check	Optional (EMV)
• Expiration Date Check	Mandatory (EMV)
Cardholder Verification	Optional (EMV) Required (VIS)
• Individual CVMs	Optional (EMV) Required (VIS)

Table 2–1: Card Functional Requirements (2 of 2)

Function	Card Support
Terminal Risk Management	Optional (EMV) Mandatory (VIS)
• Terminal Exception File	n/a (Card plays no role)
• Merchant Force Online	n/a (Card plays no role)
• Floor Limits	n/a (Card plays no role)
• Transaction Log	n/a (Card plays no role)
• Random Selection	n/a (Card plays no role)
• Velocity Checking	Optional (EMV) Not recommended but not precluded (VIS)
• New Card	Optional (VIS)
Terminal Action Analysis	IACs optional (EMV); IACs required (VIS)
Card Action Analysis	Mandatory (EMV)
• Online/offline decision	Mandatory (EMV)
• Offline referrals	Optional (EMV), Not supported (VIS)
• Card Risk Management	Optional (EMV) Mandatory (VIS) Some Card Risk Management steps are optional in VIS (refer to the *Visa Integrated Circuit Card Specification*, Chapter 11, Card Action Analysis)
• Advice Messages	Optional (EMV)
• Application Cryptogram	Algorithm option provided (EMV) Multiple algorithm options provided (VIS)
Online Processing	
• Online Capability	Mandatory (EMV)
• Issuer Authentication	Optional (EMV)
Completion	Mandatory (EMV)
Issuer-to-Card Script Processing	Optional (EMV)
• Secure Messaging	Some form is mandatory if scripts supported (EMV) Recommended form (VIS)

2.2.2 Command Support Requirements

Card support for the VSDC commands is described in Table 2–2.

Table 2–2: Command Support Requirements

Command	Card Support
APPLICATION BLOCK	Application blocking capability is optional. If supported, using APPLICATION BLOCK is recommended (VIS)
APPLICATION UNBLOCK	Application unblocking capability is optional. If supported, using APPLICATION UNBLOCK is recommended (VIS)
CARD BLOCK	Card blocking capability is recommended. CARD BLOCK command is one method (VIS)
EXTERNAL AUTHENTICATE	Conditional—If Issuer Authentication supported (EMV)
GENERATE APPLICATION CRYPTOGRAM (AC)	Mandatory (EMV)
GET CHALLENGE	Conditional—If Offline Enciphered PIN supported (EMV)
GET DATA	Optional (EMV) Mandatory (VIS)
GET PROCESSING OPTIONS	Mandatory (EMV)
INTERNAL AUTHENTICATE	Conditional—If DDA supported (EMV)
PIN CHANGE/UNBLOCK	Unblocking PIN—Optional if Offline PIN supported. Method used may be PIN CHANGE/UNBLOCK (VIS) PIN Change—Optional, must be in issuer controlled environment (VIS)
PUT DATA	Optional (VIS)
READ RECORD	Mandatory (EMV)
SELECT	Mandatory (EMV)
UPDATE RECORD	Optional (VIS)
VERIFY	Conditional—If Offline PIN supported (EMV)

Application Selection 3

Application Selection is the process of determining which of the applications that are supported by both the card and terminal will be used to conduct the transaction. This process takes place in two steps:

1. The terminal builds a candidate list of mutually supported applications.
2. A single application from this list is identified and selected to process the transaction.

This chapter is organized into the following sections:

3.1 Card Data

3.2 Terminal Data

3.3 Commands

3.4 Building the Candidate List

3.5 Identifying and Selecting the Application

3.6 Flow

3.7 Subsequent Related Processing

3.1 Card Data

The card data elements used in Application Selection are listed and briefly described in Table 3–1. For a detailed description of these elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 3–1: Application Selection—Card Data (1 of 3)

Data Element	Description
Application Identifier (AID)	The AID is composed of the Registered Application Provider Identifier (RID) and the Proprietary Application Identifier Extension (PIX). It identifies the application as described in ISO/IEC 7816-5. All Visa AIDs shall begin with a RID expressed as hexadecimal “A000000003”. The Visa RID is concatenated with a PIX representing the Visa payment type. The Visa PIXs are: 1010 Visa debit or credit 2010 Visa Electron 3010 Interlink 8010 PLUS 999910 Proprietary ATM The card AID must have a suffix if more than one application with the same AID is present on a single card. The card AID should not have a suffix if only one application with the AID is on the card unless another application with the same AID may be added to the card after personalization. A card with both a Visa credit and a Visa debit application might use the suffix as follows: A000000003101010**1**—first Visa application (Visa Credit) A000000003101010**2**—second Visa application (for Visa Debit)
Application Definition File (ADF)	A file that is the entry point to application elementary files (AEF) that contain data elements for the application. • FCI Template – DF Name – FCI Proprietary Template ▪ Application Label ▪ Application Priority Indicator (conditional. If the card contains more than one payment account, the account reflected in the magnet stripe must be priority 1.) ▪ PDOL (optional, required for geographic restrictions and VLP) ▪ Language Preference (optional) ▪ Issuer Code Table Index (optional, required if Application Preferred Name is present) ▪ Application Preferred Name (optional) ▪ FCI Issuer Discretionary Data (optional)

Table 3–1: Application Selection—Card Data (2 of 3)

Data Element	Description
Application Elementary Files (AEFs)	Application elementary files contain data elements used by the application in processing.
Application Label	Mnemonic associated with AID according to ISO/IEC 7816-5. Used in application selection. Application Label is mandatory in the File Control Information (FCI) of an Application Definition File (ADF) and in an ADF directory entry. The naming conventions for Application Label are that it shall contain “Visa” if included in the acceptance mark and shall clearly identify the payment function or product as needed to differentiate among the applications stored on the card: Visa Debit/Credit — Shall contain “Visa”. For example, “Visa”, “Visa Credit”, “Visa Debit”, or “Visa Business” Electron — Shall include “Visa” and should include “Electron”. For example, “Visa” or “Visa Electron” Interlink — Shall include “Interlink”. For example, “Interlink” or “Visa Interlink” Plus — Shall include “Plus”. For example, “Plus” or “Plus ATM”
Application Preferred Name	Mnemonic associated with AID. If the Application Preferred Name is present and the Issuer Code Table Index entry is supported by the terminal, the Application Preferred Name rather than the Application Label is displayed to the cardholder during final application selection. The Application Preferred Name should be identical to the Application Label. However, Members may use this field for their customized brand name recognizable to the customer.
Application Priority Indicator	Indicates the priority of the given application in a directory and whether the application requires cardholder confirmation to be selected.
Directory Definition File (DDF)	A file that defines the directory structure beneath it. The FCI for a DDF is as follows: • FCI Template – DF Name – FCI Proprietary Template ▪ SFI of directory ▪ FCI Issuer Discretionary Data (optional)
Directory File	A directory file is a file listing DDFs and ADFs contained within the directory. After selection, the directory is accessed with the READ RECORD command. For more detailed information on directory files, refer to the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 1*, Annex C.

Table 3–1: Application Selection—Card Data (3 of 3)

Data Element	Description
File Control Information (FCI)	Information provided in response to the SELECT command. This information varies depending on the type of file selected.
Issuer Code Table Index	Indicates the code table according to International Organisation for Standardisation (ISO) 8859 required in the terminal to display the Application Preferred Name.
Payment Systems Environment (PSE)	The PSE begins with a DDF named “1PAY.SYS.DDF01”. The directory file associated with this DDF is known as the Payment Systems Directory.
Payment Systems Directory	The Payment Systems Directory contains entries for ADFs and DDFs that are formatted according to EMV. The applications defined by the ADFs may or may not conform to EMV.
Processing Options Data Object List (PDOL)	A list of tags and lengths for terminal resident data objects needed by the card in processing the GET PROCESSING OPTIONS command during Initiate Application Processing (see Chapter 4, Initiate Application Processing, for more information).
Short File Identifier (SFI)	The SFI is a pointer to Elementary Files (EF). • 1–10 Reserved for EMV • 11–20 Payment system specific • 21–30 Issuer specific

3.2 Terminal Data

The terminal data elements described in Table 3–2 are used in Application Selection. For a detailed description of these data elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Elements Table.

Table 3–2: Application Selection—Terminal Data

Data Element	Description
Application Identifier (AID)	The AID is composed of the Registered Application Provider Identifier (RID) and the Proprietary Application Identifier Extension (PIX). It identifies the application as described in ISO/IEC 7816-5. See Table 3–1 for a list of Visa AIDs.
Application Selection Indicator	Indicates whether partial selection is supported for the AID in the terminal.
List of supported applications	The terminal shall maintain a list of applications supported by the terminal and their respective AIDs.

3.3 Commands

SELECT

The SELECT command shall be performed as described in the *EMV 4.0, Book 1*, Section 7.3.

The terminal sends the SELECT command to the card to obtain information on the applications supported by the card. The application information includes issuer preferences such as the priority in which the application is selected, application name, and language preference. The command either contains the name of the Payment Systems Environment directory (used for the directory selection method), a directory (DDF) name, or a requested AID (used for the List of AIDs method).

The P1 parameter of the command indicates that the application is being selected by name. The P2 parameter indicates whether additional applications with the same AID are being requested in support of AID suffixes (where multiple applications with the same AID are supported by the card.)

The command response may have the following SW1 SW2 return codes:

- **9000**—Successful return from SELECT
- **6A82**—Directory selection method not supported by card (command contains name of the Payment System Environment) and no file found

  6A82—Selected file not found or last file when P2 parameter specified additional applications with the same AID (command contains AID)
- **6A81**—Card is blocked or command not supported
- **6283**—Application is blocked

If the card contains a PDOL, it is part of the FCI data in the SELECT response. The terminal sends the data specified in the PDOL to the card during Initiate Application Processing.

READ RECORD

The READ RECORD command shall be performed as described in the *EMV 4.0, Book 1*, Section 7.2.

READ RECORD is used to read the records in the Payment Systems Environment directory when the directory selection method is being used. READ RECORD may only be used after selection of an ADF or DDF. The command includes the Short File Identifier (SFI) of the file to be read and the record number of the record within the file.

The card returns the requested record in the response. The SW1 SW2 response may have the following values:

- **9000**—Completed successfully
- **6A83**—Record number does not exist

3.4 Building the Candidate List

There are two approaches used by the terminal to build a list of mutually supported applications.

- Directory Selection Method is optional for cards and terminals, but if supported by the terminal, it is attempted first. In the Directory Selection Method, the terminal reads the Payment System Environment file from the card. This file is a list of all of the payment applications supported by the card. The terminal adds any applications listed in both the card list and the terminal list to the candidate list.
- List of AIDs Method is mandatory for cards and terminals. In List of AIDs Method, the terminal issues a SELECT command for each terminal-supported application. If the card response indicates that the application is supported by the card, the terminal adds the application to the candidate list.

3.4.1 Directory Selection Method

Directory Selection Method processing from a card perspective includes the following steps:

1. The card receives a SELECT command from the terminal requesting selection of the PSE (file name “1PAY.SYS.DDF01”).
   - If the card is blocked or the SELECT command is not supported, the card responds with SW1 SW2 = “6A81”.
   - If there is no PSE, the card responds to the SELECT command from the terminal indicating that this file does not exist (SW1 SW2 = “6A82”).
   - If the PSE is blocked, the card responds with “6283”.
   - If the PSE is found, the card responds to the terminal with SW1 SW2 = “9000” and the FCI for the PSE.
2. If the PSE is found, the card receives READ RECORD commands from the terminal indicating the files and records to be read. The card responds to each READ RECORD command with the requested record and SW1 SW2 = “9000”. When the requested record is not available, the card indicates this to the terminal with a response of SW1 SW2 = “6A83”.

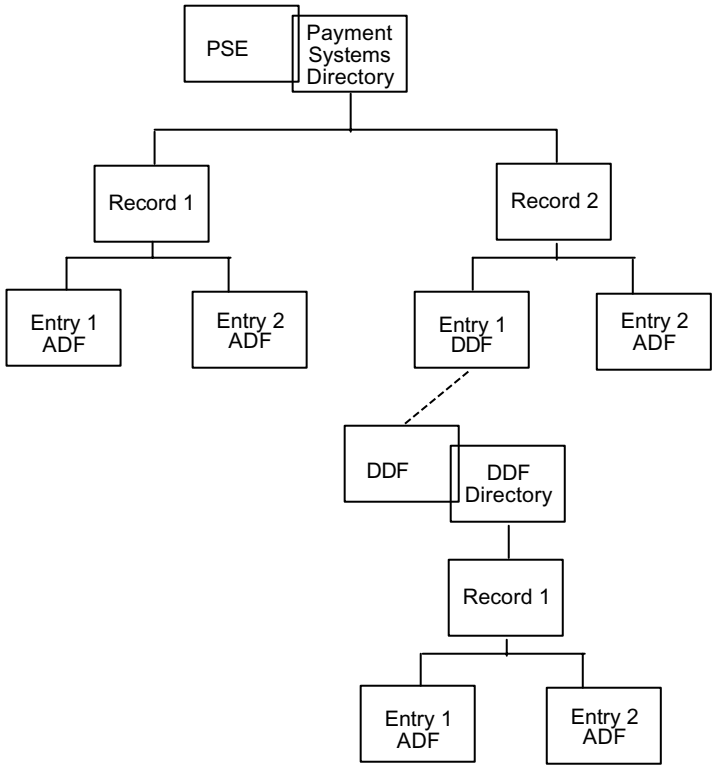
3. The terminal processes each entry in the record. If the entry represents a DDF, the terminal sends a SELECT command with the DDF name, and the card responds with the FCI for that DDF. The FCI contains the SFI for a directory file.

   The terminal requests the records contained in the directory belonging to the DDF. The card responds to each READ RECORD command with the requested record and SW1 SW2 = “9000”. When the requested record is not present, the card indicates this to the terminal with a response of SW1 SW2 = “6A83” and the terminal returns to Step 2 and continues reading the PSE.

The terminal performs the following steps, as shown in Figure 3–1:

1. Reads Record 1 from the Payment Systems Directory.
2. Checks to see if either of the AIDs for the ADF Entry 1 or 2 match terminal AIDs. If they match, they are added to the candidate list.
3. Reads Record 2 from the Payment Systems Directory.
4. SELECTs the DDF directory indicated in Entry 1 of Record 2.
5. Reads Record 3 from the DDF Directory.
6. Checks to see if either of the AIDs for the ADF Entry 1 or 2 of Record 3 match terminal AIDs. If they match, they are added to the candidate list.
7. Returns to processing entries and records from the previous directory, when card responds that there are no more records in the directory.
8. Checks to see if Entry 2, Record 2 from the Payment System Directory matches a terminal AID.
9. Completes the candidate list when the card responds that there are no more records in the Payment Systems Directory.

Figure 3–1: Sample Card Directory Structure



3.4.2 List of AIDs Method

The List of AIDs method processing from a card perspective includes the following steps:

1. The card receives the SELECT command from the terminal which includes the AID from the terminal list of supported applications. The card checks to see if any card application has a matching AID (the card AID may be longer than the terminal AID and still match).

   Sample matching AIDs are shown in Table 3–3.

Table 3–3: Sample Matching AIDs

Terminal AID	Terminal Application	Card AID	Card Application
A0000000031010	Visa	A000000003101001	Visa Debit
A0000000031010	Visa	A000000003101002	Visa Credit

   – If the AID matches, the card responds to SELECT command indicating that the application is supported by the card (SW1 SW2 = “9000”).

   – If the card does not find a matching AID, the card responds with SW1 SW2 = “6A82” indicating that the application was not found.

   – If the card is blocked or the SELECT command is not supported, the card responds with SW1 SW2 = “6A81” indicating that the transaction should be terminated.

2. If the card AID matches the terminal AID except that the card AID is longer, the card returns the entire card AID (DFname) in the SELECT command response to the terminal.

   – The card receives another SELECT command from the terminal. Parameter P2 in this SELECT is set to “02” indicating that the card should select the next application with the same terminal AID.

   – The card selects the next application with this AID and provides it to the terminal in the SELECT response.

   – When the card has no more applications with this AID, the card indicates in its response (SW1 SW2 = “6A82”) to the terminal that all matching applications have been selected.

3.5 Identifying and Selecting the Application

If there is at least one mutually supported application on the Candidate List, the terminal and cardholder determine which application to use. The terminal issues a SELECT command to the card indicating the application that has been identified for processing the transaction. The card responds to the SELECT command with SW1 SW2 = “9000” if the card determines that the transaction can be performed with that application. If the application is blocked, the card responds with SW1 SW2 = “6283”.

NOTE: *Issuers should be aware that setting their VSDC application to require confirmation by the terminal (see* EMV 4.0, Book 1, *Section 8.3.4) will mean that the application cannot be selected by a terminal that does not support either Cardholder Confirmation or Cardholder Selection.*

3.6 Flow

Figure 3–2: Application Selection Using Directory Method

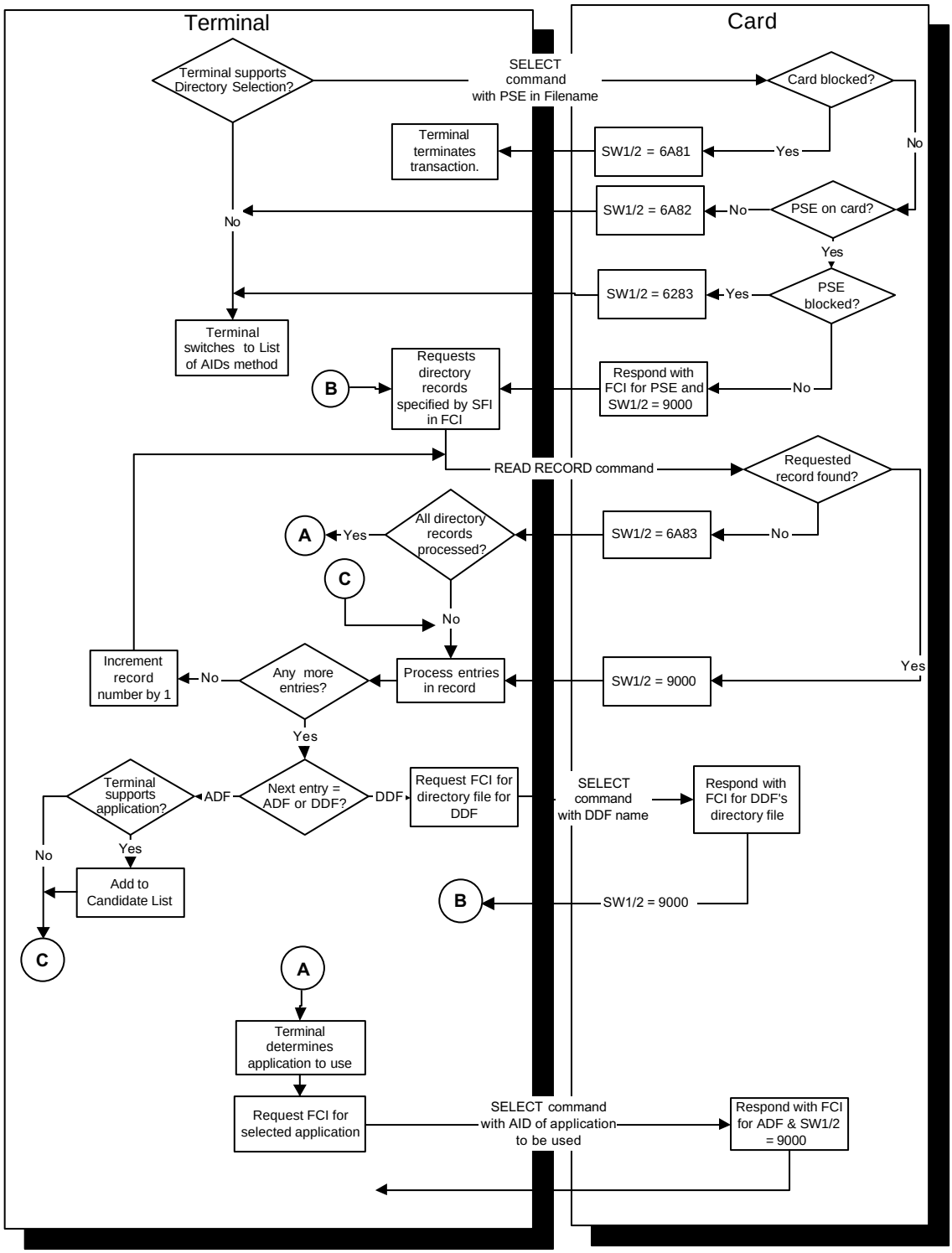
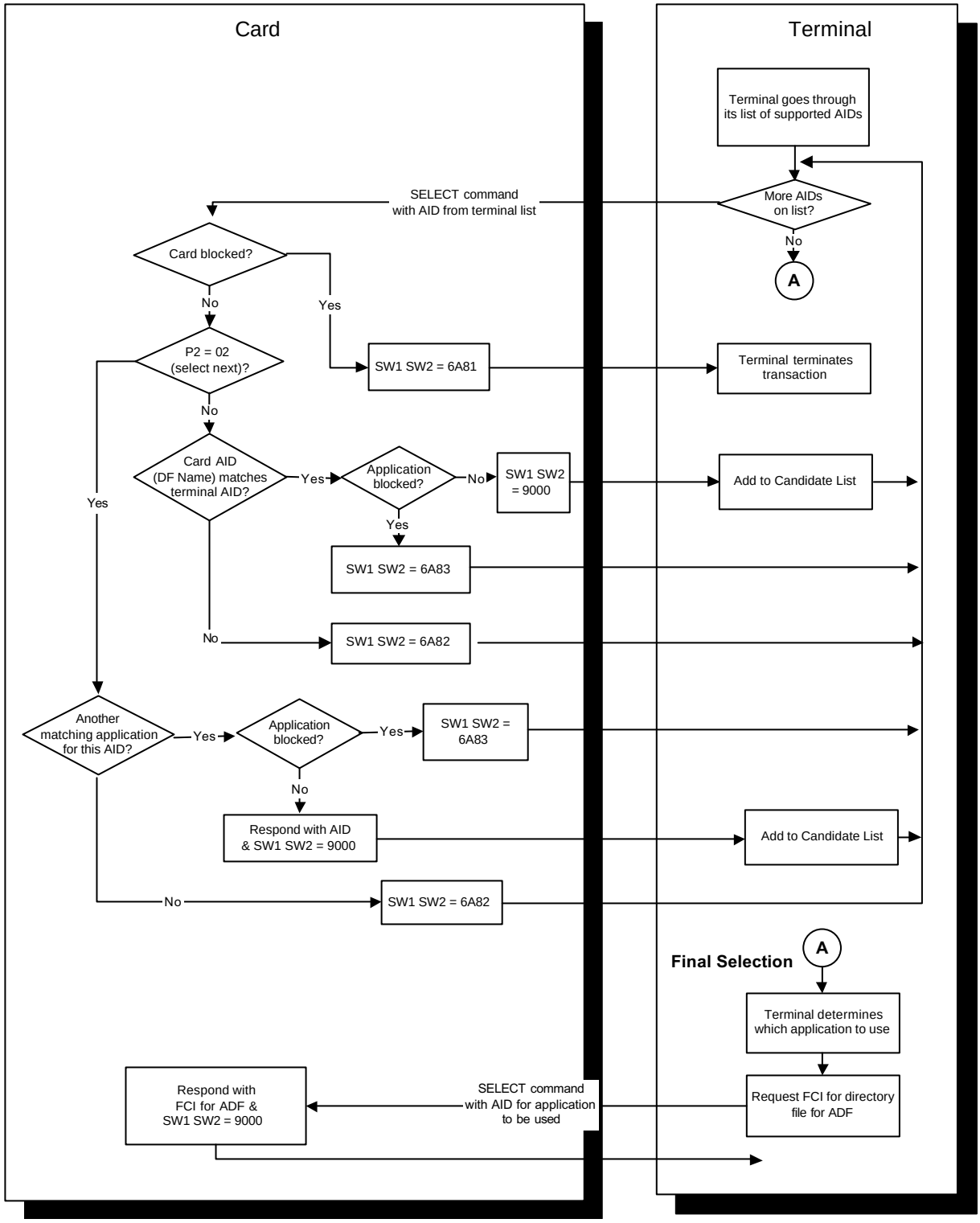


Figure 3–3: Application Selection Using List of AIDs



3.7 Subsequent Related Processing

Initiate Application Processing

The GET PROCESSING OPTIONS command sent to the card by the terminal includes any terminal data specified in the PDOL. If supported, the PDOL was included in the SELECT response during Application Selection.

If geographic restrictions or other restrictions do not permit the selected application to be initiated, the terminal terminates that application and returns to Application Selection for selection of another application.

Initiate Application Processing 4

During Initiate Application Processing, the terminal signals to the card that transaction processing is beginning. The terminal accomplishes this by sending the GET PROCESSING OPTIONS command to the card. When issuing this command, the terminal supplies the card with any data elements requested by the card in the Processing Options Data Objects List (PDOL). The PDOL (a list of tags and lengths of data elements) is optionally provided by the card to the terminal during Application Selection.

The card responds to the GET PROCESSING OPTIONS command with the Application Interchange Profile (AIP), a list of functions to be performed in processing the transaction. The card also provides the Application File Locator (AFL), a list of files and records that the terminal needs to read from the card.

Initiate Application Processing shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 6.1, and *Book 4*, Section 2.3.1.

This chapter is organized into the following sections:

4.1 Card Data

4.2 Terminal Data

4.3 GET PROCESSING OPTIONS Command

4.4 Processing

4.5 Prior Related Processing

4.6 Subsequent Related Processing

4.1 Card Data

The card data elements used in Initiate Application Processing are listed and described in Table 4–1. For a detailed description of these data elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 4–1: Initiate Application Processing—Card Data (1 of 2)

Data Element	Description
Application File Locator (AFL)	Indicates the file location and range of records which contain card data to be read by the terminal for use in transaction processing. For each file to be read, the AFL contains the following information: • Byte 1—Short File Identifier (a numeric label file) • Byte 2—Record number of the first record to be read • Byte 3—Record number of the last record to be read • Byte 4—Number of consecutive records containing data to be used in Offline Data Authentication beginning with the first record to be read as indicated in Byte 2.
Application Interchange Profile (AIP)	A list that indicates the capability of the card to support specific functions in the application (SDA, Standard DDA, Combined DDA/Generate AC, Terminal Risk Management, Cardholder Verification, and Issuer Authentication). The AIP must be personalized in the card to indicate support for Terminal Risk Management and Cardholder Verification.
Application Transaction Counter (ATC)	Counter of transactions initiated for the card application since the application was personalized.
Card Verification Results (CVR)	Visa proprietary data element that indicates the results of offline processing from current and previous transactions from a card perspective. This data is stored in the card and transmitted online as part of the Issuer Application Data.
Cryptogram Information Data (CID)	Indicates the type of cryptogram returned by the card and the subsequent actions to be performed by the terminal. Initialized to zeros during Initiate Application Processing.
Geographic Indicator	Visa proprietary data element that indicates whether a transaction is valid for domestic and international transactions. This data element is required if the Geographic Restrictions check described in Section 4.4 Processing, is supported.

Table 4–1: Initiate Application Processing—Card Data (2 of 2)

Data Element	Description
Issuer Country Code	Visa proprietary data element indicating the issuer's country code. The Issuer Country Code (Tag "9F57") is stored in a proprietary file internal to the card. This data element is required if the Geographic Restrictions check is supported.
Processing Options Data Object List (PDOL)	The PDOL is a list of tags and lengths for terminal-resident data objects needed by the card in processing the GET PROCESSING OPTIONS command during Initiate Application Processing (Chapter 3, Application Selection).

4.2 Terminal Data

The terminal data elements used in Initiate Application Processing are listed and described in Table 4–2. For a detailed description of these data elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Elements Table.

Table 4–2: Initiate Application Processing—Terminal Data

Data Element	Description
Terminal Country Code	Terminal data indicating the country of the terminal. It is provided to the card in the GET PROCESSING OPTIONS command if specified in the PDOL previously received from the card.
Other data specified in the PDOL	The data from the terminal includes any other data specified in the card's PDOL.

4.3 GET PROCESSING OPTIONS Command

The GET PROCESSING OPTIONS command is used by the terminal to signal the card that transaction processing is beginning.

The command contains the value portion of terminal data elements requested by the card in the Processing Options Data Objects List (PDOL) that was optionally provided by the card during Application Selection.

The card response is in Format 1 and is described in the *EMV 4.0, Book 3*, Section 2.5.8. It contains the Application Interchange Profile (AIP) specifying the functions supported by the card and the Application File Locator (AFL) specifying the files and records to be used for the transaction.

4.4 Processing

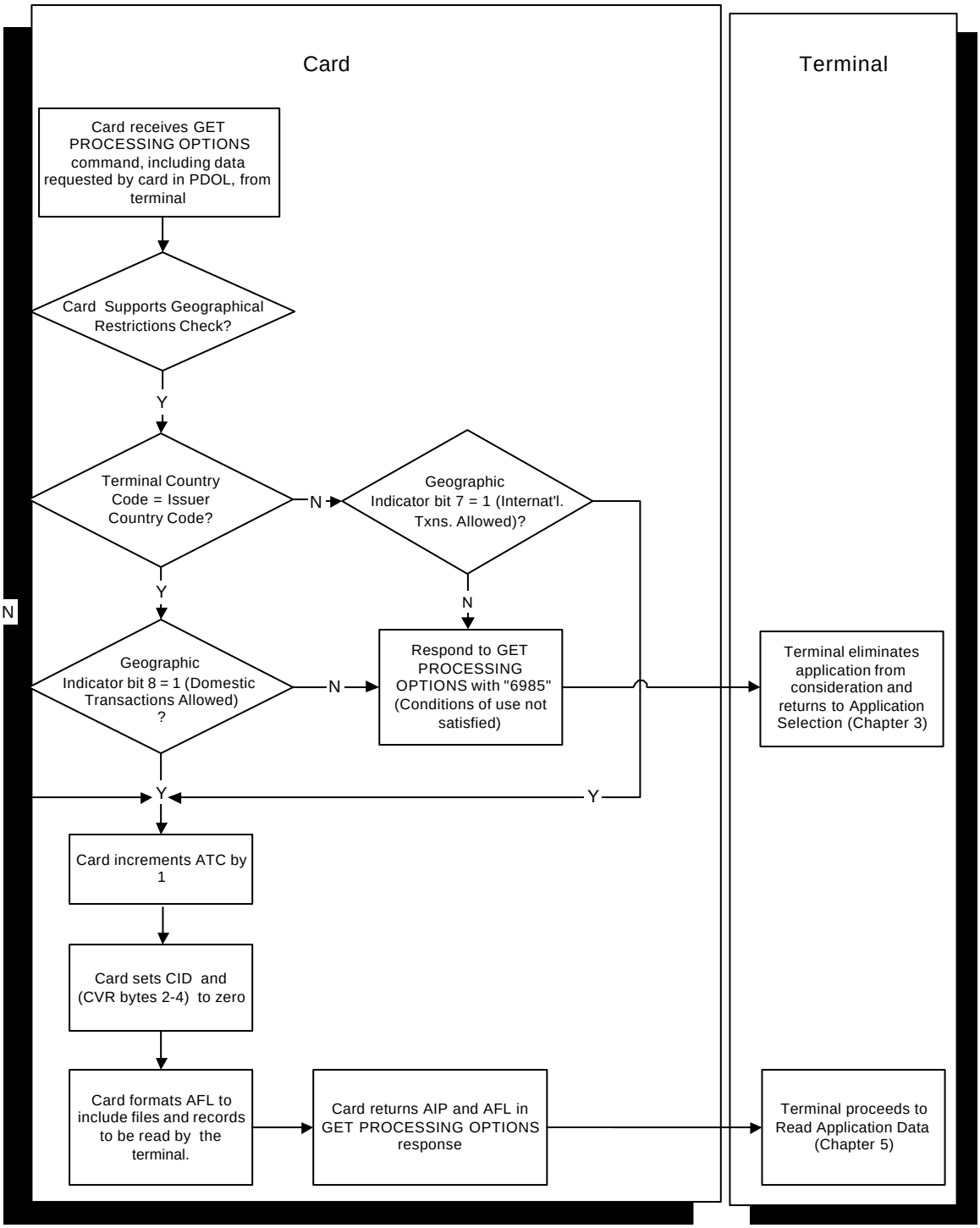
After receiving a GET PROCESSING OPTIONS command from the terminal, the card:

1. Performs the Geographic Restrictions check if supported:
   a. Compares Terminal Country Code to Issuer Country Code (tag “9F57”) to determine whether the transaction is international or domestic.
   b. Checks the Geographic Indicator if present.
      - If the transaction is domestic and bit 8 of the Geographic Indicator is “0”, the transaction is not allowed.
      - If the transaction is international and bit 7 of the Geographic Indicator is “0”, the transaction is not allowed.
   c. If Geographic Restrictions apply, the card responds to the GET PROCESSING OPTIONS command with an error code “Conditions of use not satisfied” (SW1 SW2 = “6985”) indicating that the terminal shall eliminate the current application from consideration and return to Application Selection to select another application. In addition to Geographic Restrictions, issuer proprietary checks may set SW1 SW2 to “6985” to cause a return to Application Selection.
2. Determines the files and records that are to be read and locates or builds the AFL. Additional proprietary checks may be used to initiate customized processing by designating different AIPs and AFLs for different conditions. For example, AFLs designating different Cardholder Verification Method (CVM) Lists could be used for domestic and international transactions. Appendix G describes the customized processing necessary to support the Visa Low-value Payment option.

3. If no Geographic Restrictions or proprietary restrictions apply, the card:
   a. Increments the Application Transaction Counter (ATC) by 1
   b. Sets Cryptogram Information Data (CID) to zero
   c. Sets Card Verification Results (CVR) to zero (except for the length indicator)
   d. Responds to the GET PROCESSING OPTIONS command with the AIP and the AFL

The Initiate Application Processing flow is shown in Figure 4–1.

Figure 4–1: Initiate Application Processing Flow



4.5 Prior Related Processing

Application Selection

The card supplies the PDOL (if present) to the terminal as part of the FCI provided in response to the SELECT command.

4.6 Subsequent Related Processing

Application Selection

If Geographic Restrictions or other restrictions applied and control was returned to Application Selection, the application is removed from the list of eligible applications and selection of another application is allowed.

Read Application Data

The AFL provided by the card in response to the GET PROCESSING OPTIONS command is used by the terminal to determine what application data to read from the card and which data is to be used in Offline Data Authentication.

Offline Data Authentication

The terminal uses the AIP provided by the card in response to the GET PROCESSING OPTIONS command to determine the forms of Offline Data Authentication supported by the card.

Cardholder Verification

The terminal uses the AIP provided by the card in response to the GET PROCESSING OPTIONS command to determine if the card supports Cardholder Verification.

Online Processing

The terminal uses the AIP provided by the card in response to the GET PROCESSING OPTIONS command to determine if the card supports Issuer Authentication.

Read Application Data 5

During Read Application Data, the terminal reads the card data necessary to process the transaction and determines the data to be authenticated during SDA or DDA.

Read Application Data shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3,* Section 6.2.

This chapter is organized into the following sections:

5.1 Card Data

5.2 Terminal Data

5.3 READ RECORD Command

5.4 Processing

5.5 Prior Related Processing

5.6 Subsequent Related Processing

5.1 Card Data

Appendix A, Card and Issuer Data Element Tables, contains detailed descriptions of the card data elements and their usage.

The data element described in Table 5–1 was previously sent from the card to the terminal during Initiate Application Processing and is used during Read Application Data.

Table 5–1: Read Application Data—Card Data

Data Element	Description
Application File Locator (AFL)	During the Initiate Application Processing function, the card sends the terminal the AFL which contains an entry for group of records to be read. Each entry designates • The Short File Identifier (SFI) of the file • The record numbers of the first record and last record to read from the file • The number of records beginning with the first record read in the file to be used for authentication during Static Data Authentication (SDA) and Dynamic Data Authentication (DDA).

Read Application Data reads records from the card's Application Elementary Files described in Table 5–2.

Table 5–2: Read Application Data—Card Files

Data Element	Description
Application Elementary Files (AEF)	Card data files containing data used for application processing. An AEF consists of a sequence of records which are addressed by record number. Each AEF is identified by a unique Short File Identifier (SFI). The terminal reads these records using the READ RECORD command containing a designation of the SFI and record number to be read.
Short File Identifier (SFI)	The SFI is a number used to uniquely identify application data files. It is listed in the AFL and used by the terminal to identify the files to be read.

5.2 Terminal Data

The card uses no terminal data in Read Application Data.

5.3 READ RECORD Command

The READ RECORD command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.11.

The command received from the terminal includes the Short File Identifier (SFI) of the file to be read and the record number of the record within the file.

The command response returned by the card shall include the requested record in the data field.

5.4 Processing

The card receives the READ RECORD command from the terminal and returns the requested record to the terminal. A READ RECORD command is received for each record designated in the AFL.

The terminal continues to issue READ RECORD commands until all designated records within each designated file have been read.

5.5 Prior Related Processing

Initiate Application Processing

During Initiate Application Processing, the card sends the AFL to the terminal to designate the records the terminal should request from the card.

5.6 Subsequent Related Processing

Other functions use the data read during Read Application Data.

Offline Data Authentication

The terminal uses the list of static data to be authenticated that is built during Read Application Data for the validation of the Signed Static Application Data during SDA or the ICC Public Key Certificate during DDA.

Offline Data Authentication 6

Offline Data Authentication is the process by which the terminal authenticates data from the card using RSA public key technology. Offline Data Authentication has two forms:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)

During SDA processing the terminal authenticates static (unchanging) data from the card. SDA ensures that issuer-selected card data elements have not been changed since the card was personalized.

DDA can be either Standard DDA or Combined DDA/AC Generation. During DDA processing the terminal authenticates the static card data and also authenticates a cryptogram that the card generates using transaction-unique data. DDA ensures that issuer-selected card data elements have not been altered since the card was personalized. DDA also confirms that the card is genuine and has not been created by copying data from a valid card to a counterfeit card (skimming).

Offline Data Authentication results are considered in the card and terminal's decision of whether to approve offline, go online for authorization, or decline offline. Online authorization systems may use the results of Offline Data Authentication in their authorization response decision.

Offline Data Authentication shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 2,* Sections 5 and 6. Offline Data Authentication must be supported by all offline capable terminals. Offline Data Authentication support is optional for cards.

This chapter is organized into the following sections:

6.1 Keys and Certificates

6.2 Determining Whether to Perform SDA or DDA

6.3 Static Data Authentication (SDA)

6.4 Dynamic Data Authentication (DDA)

6.5 Prior Related Processing

6.6 Subsequent Related Processing

6.1 Keys and Certificates

Offline Data Authentication is performed by the terminal using RSA public key technology to validate digital certificates and signatures from the card. RSA public key technology uses private keys to generate enciphered values (certificates or signatures) of data elements which are later decrypted (unlocked) for validation and data recovery. For additional information on the RSA algorithm, refer to the *EMV 4.0, Book 2*, Annex B2.1.

6.1.1 Visa Certificate Authority (CA)

Offline Data Authentication requires a Certificate Authority (CA) which is a highly secure cryptographic facility that signs the issuer's public keys with the Visa CA Private Keys. Terminals contain the CA public keys for the applications recognized by the terminal. Visa is the Certificate Authority for Visa Smart Debit and Visa Smart Credit applications.

The issuer services provided by the Visa CA are:

- Generation of all Visa CA RSA key pairs.
- Generation of Issuer Public Key (PK) Certificates from public keys provided by issuers.
- Performance of all key management processes required to support the generation of Issuer PK Certificates.
- Administration of certificate revocation procedures as outlined by the *EMV 4.0, Book 2*, Section 10.

6.1.2 RSA Key Pairs

Three key pairs are involved in Offline Data Authentication:

- Visa CA Public/Private Keys (SDA and DDA)
- Issuer Public/Private Keys (SDA and DDA)
- ICC Public/Private Keys (DDA only)

6.1.2.1 Visa Public/Private Keys

Visa as a CA generates up to six RSA public/private key pairs. Each key pair is identified by a unique Public Key Index (PKI). The Visa CA Public Keys and their indexes are loaded into terminals by acquirers. The Visa Private Keys are kept secret and used to sign Issuer Public Keys. The same Visa public/ private key pairs are used for SDA, DDA, and Offline Enciphered PIN.

Visa may periodically withdraw a public key pair or introduce a new key pair.

An expiration date is assigned to each certificate. The application's expiration date shall not be greater than the expiration date of the certificate.

Issuers shall support EMV and Visa requirements for revocation and introduction of Visa CA Public Keys. The EMV requirements are listed in the *EMV 4.0, Book 2*, Section 10.

6.1.2.2 Issuer Public/Private Keys

To support SDA or DDA the issuer shall generate one or more RSA public/private key pair within a Host Security Module (HSM) and obtain Issuer PK Certificates from the Visa CA.

The Issuer Private Keys shall be kept in a secure device to be used to encrypt data for the card personalization process.

The Issuer Public Key is stored in an Issuer PK Certificate on the card. To obtain Issuer PK Certificates to personalize on cards:

- The issuer sends the Issuer Public Key to Visa.
- The Visa CA creates one or more Issuer PK Certificates with Visa Private Keys. An Issuer PK Certificate is created for each Visa CA Public Key which is equal to or longer than the Issuer Public Key and which expires after the expiration date of the Issuer PK Certificate. An Issuer PK Certificate is created by signing the issuer's Public Key input file with the Visa CA private key.
- The Certificate Authority Public Key Index (PKI) of the signing key is associated with the Issuer PK Certificate.
- The Issuer PK Certificates and associated PKIs are conveyed to the issuer from the Visa CA.

This process is described in the *Visa Certificate Authority User's Guide*.

The format of the data recovered from Issuer PK Certificate is shown in the *EMV 4.0, Book 2*, Table 4. The following is a partial list of data elements in the Issuer PK Certificate:

- Certificate Expiration Date assigned by the issuer
- The Issuer Public Key or the leftmost digits of the Issuer Public Key if the entire key does not fit in the certificate
- The Issuer Public Key Length which shall be shorter than or equal to the Visa CA Public Key length
- The hash result from hashing the Issuer Public Key and other data elements specified in the *EMV 4.0, Book 2*, Table 1.

All cards which support SDA or DDA shall be personalized with an Issuer PK Certificate and a CA Public Key Index (PKI) to identify the Visa Public Key to use to decrypt the certificate.

The same Issuer Public/Private Keys and Issuer PK Certificates are used for both SDA and DDA.

6.1.2.3 ICC Public/Private Keys

For cards supporting DDA, the issuer shall generate a unique ICC public/private key pair for each card.

The ICC Private Key shall be stored in a secure location in the card.

The ICC Public Key is included in the ICC Public Key (PK) Certificate which is encrypted with the Issuer Private Key. The ICC PK Certificate is personalized on the card. The ICC PK Certificate format and a complete list of the certificate subfields are shown in the *EMV 4.0, Book 2*, Table 10. The following is a partial list of the data elements included in the certificate:

- Certificate Expiration Date
- ICC Public Key or the leftmost digits of the key if the entire key does not completely fit in the certificate
- ICC Public Key length which must be shorter than or equal to the Issuer Public Key length
- The hash result from the hash of the ICC Public Key and related information including the static data to be authenticated. The data to be hashed is shown in the *EMV 4.0, Book 2*, Table 11.

The ICC public/private key data may also be used to support the Offline Enciphered PIN method of cardholder verification described in Chapter 8, Cardholder Verification.

6.2 Determining Whether to Perform SDA or DDA

The terminal uses the card's Application Interchange Profile (AIP) and the offline data authentication support provided by the terminal to determine whether to perform SDA, Standard DDA, or Combined DDA/AC Generation.

6.2.1 Card Data

The terminal uses the data from the card, described in Table 6–1, to determine whether to perform SDA or DDA.

Table 6–1: Offline Data Authentication—Card Data

Data Element	Description
Application Interchange Profile (AIP)	Contains indicators for: • Static Data Authentication is supported by card • Dynamic Data Authentication is supported by card • Combined DDA/AC Generation is supported by card

6.2.2 Processing

Only one method of offline data authentication is performed during a transaction. Combined DDA/AC Generation receives priority over Standard DDA, and Standard DDA receives priority over SDA. If the card and terminal do not support a common offline data authentication method, no offline data authentication is done.

If the terminal determines that both the card (as indicated by the AIP) and terminal support Combined DDA/AC Generation, it performs Combined DDA/AC Generation. Otherwise, if both support Standard DDA, the terminal performs Standard DDA. Otherwise, if both card and terminal support SDA, the terminal performs SDA.

6.3 Static Data Authentication (SDA)

During SDA processing, the terminal uses RSA public key verification technology to validate that key data elements on the card have not been altered since card personalization.

6.3.1 Card Data

The terminal uses the card data elements described in Table 6–2 in SDA processing or in processing related to SDA processing. Appendix A, Card and Issuer Data Element Tables, contains detailed descriptions of the card data elements and their usage.

Table 6–2: Card Data Used in SDA (1 of 2)

Data Element	Description
Certificate Authority Public Key Index (PKI)	Provided by the CA with the Issuer PK Certificate. It identifies the payment scheme public key in the terminal to use for verifying the Issuer PK Certificate.
Issuer Public Key Certificate	The certificate containing the Issuer Public Key that has been signed with the Visa CA Private Key. This certificate is described in the Issuer Public/Private Keys section of this chapter.
Issuer Public Key Exponent	The exponent used in the RSA algorithm to recover the Issuer PK Certificate. The Issuer Public Key exponent shall be 3 or 2^{16} + 1.
Issuer Public Key Remainder	The portion, if any, of the Issuer Public Key that does not fit into the Issuer PK Certificate.
Registered Application Identifier (RID) portion of the Application Identifier (AID)	The RID is registered with International Organisation for Standardisation (ISO) and identifies the payment scheme specific list of public keys that is stored in the terminal. Visa's RID is "A000000003".

Table 6–2: Card Data Used in SDA (2 of 2)

Data Element	Description
Signed Static Application Data (SAD)	A signature used in the validation of the card's static data. The SAD is signed with the Issuer Private Key and is placed on the card during the personalization process. The format of the SAD is shown in the *EMV 4.0, Book 2*, Table 5. The format of the data elements to be hashed are in the same EMV document in Table 2. The following data elements are recommended for inclusion in the signature generation: • Application Interchange Profile if either method of DDA is supported • Application Effective Date • Application Expiration Date • Application PAN • Application PAN Sequence Number • Application Usage Control • Cardholder Verification Method (CVM) List • Issuer Action Code—Default • Issuer Action Code—Denial • Issuer Action Code—Online • Issuer Country Code ("5F28") If the signed data is not unique within the application, multiple SADs must be supported. An example of when this data might not be unique is when a card has different CVM Lists for domestic and international transactions and the CVM List is used in the signature. See Chapter 4, Initiate Application Processing, for an explanation of the Geographic Restrictions check and how different data can be specified. If the card supports the ability to change any of the signed data elements after the card has been issued to the cardholder, the capability to change the SAD shall also be supported.
SDA Tag List	Contains the tag of the Application Interchange Profile (AIP) if it is to be signed. Tags other than the tag of the AIP shall not be present in the SDA Tag List. The AIP is recommended for inclusion in the SDA Tag List if either method of DDA is supported.

The card uses the data element described in Table 6–3 in processing related to SDA.

Table 6–3: Offline Data Authentication—SDA Related Card Data

Data Element	Description
Card Verification Results (CVR)	Contains an indicator that is set during Card Action Analysis of subsequent transactions showing that SDA failed on a previous offline-declined transaction.
SDA Failure Indicator	If SDA fails and the transaction is declined offline, this indicator is set during Card Action Analysis. It is reset during Completion of a subsequent online transaction based upon Issuer Authentication conditions.

6.3.2 Terminal Data

The card uses no terminal data during SDA.

6.3.3 Commands

No commands are utilized in SDA processing.

6.3.4 Processing

The card performs no processing during SDA.

During SDA, the terminal uses RSA public key verification technology to recover and validate the Issuer Public Key and to validate the SAD from the card. The terminal's SDA processing steps are described in more detail in the Terminal volume of this document and in the *EMV 4.0, Book 2*, Chapter 5, and are summarized below:

1. Retrieval of the CA Public Key

   The terminal uses the PKI and the RID from the card to determine which Visa CA Public Key to use.

2. Retrieval of the Issuer Public Key

   The terminal uses the Visa CA Public Key to unlock the Issuer PK Certificate and recover the Issuer Public Key.

3. Verification of Signed Static Application Data

   a. Recover hash value—The terminal uses the Issuer Public Key to verify the SAD to obtain the hash of the signed data elements. This hash was generated for card personalization by concatenating key data elements and using a hashing algorithm to convert them into a single data element.

   b. Calculate hash value—The terminal calculates a hash value using data elements which were previously read in the clear from the card and designated in the Application File Locator (AFL) and Static Data Authentication Tag List.

   c. Compare hash values—The terminal verifies that the hash recovered from the signature matches the hash calculated from the cleartext card data.

If all of the SDA steps are successful, SDA has passed.

6.4 Dynamic Data Authentication (DDA)

During DDA processing, the terminal uses RSA public key technology to determine whether key data elements from the card have been altered since card personalization and whether the card is counterfeit.

VIS supports two forms of Dynamic Data Authentication: Standard DDA and Combined DDA/AC Generation. With both, the terminal validates that static card data has not been altered and also validates a dynamic cryptogram generated by the card. With Standard DDA, the card generates the dynamic signature using dynamic terminal, card, and transaction data in response to an INTERNAL AUTHENTICATE command received prior to Card Action Analysis. With Combined DDA/AC Generation, the card responds to the first GENERATE AC command received during Card Action Analysis by generating a dynamic signature that includes the Application Cryptogram and Cryptogram Information Data as well as the dynamic terminal, card, and transaction data used for Standard DDA.

6.4.1 Card Data

Appendix A, Card and Issuer Data Element Tables, contains detailed descriptions of the card data elements and their usage. Except for the SAD, all of the card data elements used by the terminal in SDA are also used in DDA. The card data described in Table 6–4 is used for DDA only.

Table 6–4: Offline Data Authentication—DDA Card Data (1 of 2)

Data Element	Description
Dynamic Data Authentication Data Object List (DDOL)	The list the card provides the terminal that specifies the terminal data elements the terminal must include in the INTERNAL AUTHENTICATE command. The card includes these terminal data elements in the hash in the Signed Dynamic Application Data. At a minimum, the DDOL shall contain the tag for the Unpredictable Number (tag “9F37”).
ICC Dynamic Data	Issuer-specified data elements to be included in the Signed Dynamic Application Data. Visa mandates that the Application Transaction Counter (ATC) be the first data element of the ICC Dynamic Data.
ICC Dynamic Number	Part of the ICC Dynamic Data containing time-variant number generated by the ICC
ICC Public Key (PK) Certificate	A certificate containing the ICC Public Key and a hash of static card data elements. The ICC PK Certificate is created using the Issuer Private Key and placed on the card during card personalization. This ICC PK Certificate is further described in the ICC Public/Private Key section of this chapter. The static data elements used in the ICC PK Certificate hash are the same data elements used to generate the card’s SAD used in SDA. These data elements are specified by the AFL and in the SDA Tag List during Read Application Data. If the static data is not unique within the application, multiple ICC PK Certificates must be supported. An example of when this data might not be unique is when a card uses different CVM Lists for domestic and international transactions. See Chapter 4, Initiate Application Processing, Section 4.4 Processing for additional information. If any of the signed data elements can be changed post-issuance, the capability to change the ICC Public Key Certificate and the hash of static data within it must also be supported.
ICC Public Key Exponent	The exponent to be used in the RSA recovery of the Signed Dynamic Application Data. The ICC Public Key exponent shall be 3 or 2^{16} + 1.

Table 6–4: Offline Data Authentication—DDA Card Data (2 of 2)

Data Element	Description
ICC Public Key Remainder	The portion, if any, of the ICC Public Key that does not fit into the ICC Public Key Certificate.
Signed Dynamic Application Data	The signature generated by the card at transaction time after receipt of the INTERNAL AUTHENTICATE command. The card generates this signature using a hash of dynamic data from the terminal and card. The card signs the Signed Dynamic Application Data with the ICC Private Key. The format of the Signed Dynamic Application Data is shown in the *EMV 4.0, Book 2*, Table 13.

During DDA processing, the card uses the data elements described in Table 6–5 which are not passed to the terminal.

Table 6–5: Offline Data Authentication—Internal Card Data Used During DDA

Data Element	Description
Card Verification Results (CVR)	Contains the following indicators related to DDA: • Offline Dynamic Data Authentication Failed on Last Transaction and Transaction Declined Offline • Offline Dynamic Data Authentication Performed
ICC Private Key	The key used to encrypt the Signed Dynamic Application Data.
DDA Failure Indicator	Indicates that DDA failed on a previous transaction that was declined offline. It is reset during the Completion step of a subsequent online transaction based upon Issuer Authentication conditions.

6.4.2 Terminal Data

The card uses the data from the terminal, described in Table 6–6, during DDA processing. The *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables, contains detailed descriptions of the terminal data elements and their usage.

Table 6–6: Offline Data Authentication—DDA Terminal Data

Data Element	Description
Unpredictable Number and other data specified by the card in the DDOL	This data is included in the INTERNAL AUTHENTICATE command.
Default Dynamic Data Object List	Used as the DDOL if the card does not contain a DDOL.

6.4.3 Commands

6.4.3.1 INTERNAL AUTHENTICATE Command

The terminal issues the INTERNAL AUTHENTICATE command during Standard DDA processing. The command includes the terminal dynamic data specified in the DDOL or Default DDOL.

When the card receives the INTERNAL AUTHENTICATE command, it generates the Signed Dynamic Application Data which it signs with the ICC Private Key. This dynamic signature is included in the INTERNAL AUTHENTICATE command response.

6.4.3.2 GENERATE APPLICATION CRYPTOGRAM (AC) Command

The terminal issues the first GENERATE AC command during Card Action Analysis processing. The transaction is eligible for Combined DDA/AC Generation if either:

- The card's CDOL1 specifies Terminal Capabilities and Terminal Capabilities passed in the GENERATE AC data shows that Combined DDA/AC Generation is supported and the Application Interchange Profile (AIP) shows card support for Combined DDA/AC Generation
- The CDOL1 does not specify Terminal Capabilities and bit 6 of the P1 byte is set to "1" indicating Combined DDA/AC Generation eligibility

If the transaction is eligible for Combined DDA/AC Generation, a TC or ARQC returned by the card shall be contained within the DDA cryptographic envelope as described in the *EMV 4.0, Book 2*, Section 6.6.1. See Chapter 11 for additional information on this command.

6.4.4 Processing

During DDA processing, the terminal uses RSA public key technology to validate the Issuer PK Certificate, the ICC PK Certificate and the Signed Dynamic Application Data (the dynamic signature) from the card.

The only function performed by the card during DDA processing is the generation of the dynamic signature.

DDA processing is described in more detail in the *Visa Integrated Circuit Card Terminal Specification* and in the *EMV 4.0, Book 2*, Section 6, *Book 3*, Section 6.3, and *Book 4*, Section 2.3.2. The following sections provide an overview of the Standard DDA and Combined DDA/AC Generation processes.

6.4.4.1 Standard DDA

Standard DDA processing requires the following steps:

1. Retrieval of CA Public Key

   The terminal uses the Registered Application Provider Identifier (RID) and the CA Public Key Index (PKI) to locate the Visa CA Public Key to be used for DDA.

2. Retrieval of Issuer Public Key

   The terminal uses the Visa CA Public Key to unlock the Issuer PK Certificate to recover the Issuer Public Key.

3. Retrieval of ICC Public Key

   The terminal uses the Issuer Public Key to unlock the ICC PK Certificate and recover the ICC Public Key and the hash of static data. This certificate guarantees the legitimacy of the ICC Public Key. The terminal recalculates the static data hash using the actual data elements received in the clear from the card earlier in the transaction and checks that the calculated hash matches the recovered hash.

4. Dynamic Signature Generation (Standard DDA only)

   The terminal sends the card an INTERNAL AUTHENTICATE command requesting a dynamic signature. This command includes the data requested by the card in the DDOL.

   Upon receiving the INTERNAL AUTHENTICATE command, the card shall:

   a. Set the Offline Dynamic Data Authentication Performed bit to "1" in the Card Verification Results (CVR).

   b. Concatenate the terminal data received in the INTERNAL AUTHENTICATE command and the card data specified in the ICC Dynamic Data with other data. The *EMV 4.0, Book 2*, Table 11, shows the format of the concatenation.

   c. Generate a hash value from the data concatenated above.

   d. Include the hash in the Signed Dynamic Application Data.

   e. Sign the Signed Dynamic Application Data with the ICC Private Key.

   f. Return the Signed Dynamic Application Data to the terminal in the INTERNAL AUTHENTICATE response.

5. Dynamic Signature Verification (Standard DDA only)

   To validate the dynamic signature, the terminal does the following:

   a. Uses the ICC Public Key to unlock the dynamic signature (Signed Dynamic Application Data) and recover the hash of data elements.

   b. Calculates a hash from the dynamic data elements which are in the clear.

   c. Checks that the calculated hash matches the hash recovered from the Signed Dynamic Application Data.

If all of the above steps are successful, Standard DDA has passed.

6.4.4.2 Combined DDA/AC Generation

Combined DDA/AC Generation requires the following processing:

- The terminal performs Steps 1 to 3 of Standard DDA processing after Read Application Data and prior to Terminal Action Analysis.
- The remaining card step of Combined DDA/AC Generation is the generation of the dynamic signature containing the Application Cryptogram. This step occurs when the first GENERATE AC is received during Card Action Analysis and is described in Chapter 11. This inclusion of the Application Cryptogram in a dynamic signature only occurs when the transaction is eligible for Combined DDA/AC Generation as shown in the GENERATE AC command and the Application Cryptogram is an ARQC or TC.
- The remaining terminal step of Combined DDA/AC Generation is the validation of the dynamic signature which occurs during Online Processing and is described in Chapter 12 of the Terminal Volume. If the validation of the dynamic signature fails, the transaction is declined offline.

6.5 Prior Related Processing

Read Application Data

The terminal reads the application data from the card. For cards supporting SDA, this data includes the Issuer PK Certificate, other key-related data, and the Signed Static Authentication Data (SAD). For cards supporting DDA, the DDOL, ICC PK Certificate, and other ICC key-related data are also included. A list of static data to be authenticated is built from the AFL indicators showing the records involved in offline data authentication and from the Static Data Authentication Tag List.

6.6 Subsequent Related Processing

Terminal Action Analysis

The terminal uses SDA and DDA results and card and terminal parameters to determine whether the transaction should be declined offline, sent online for authorization, or approved offline.

Card Action Analysis

If the transaction is eligible for Combined DDA/AC Generation, the card puts ARQC and TC responses in an RSA envelope prior to responding to the terminal.

If the Dynamic Data Authentication Failure indicator is set to “1”, the card sets the Dynamic Data Authentication Failed on Last Transaction and Transaction was Declined Offline bit to “1” in the CVR. A similar indicator is set if the Static Data Authentication Failure indicator is set to “1”.

If the current transaction is declined offline and the Dynamic Data Authentication Failed bit is set to “1” in the TVR received from the terminal, the card sets the Dynamic Data Authentication Failure indicator to “1”. Similar indicators are set for SDA.

Online Processing

If Combined DDA/AC Generation is the offline data authentication method and the card response to the first GENERATE AC is a TC or ARQC, the terminal recovers and validates the data in the RSA signature envelope in the GENERATE AC response.

Completion

The Static Data Authentication Failure and Dynamic Data Authentication Failure indicators are reset to “0” when the transaction is processed online and Issuer Authentication is:

- Performed and passed
- Supported, optional (as shown in the Issuer Authentication Indicator), and not performed, or
- Not supported (as shown in the Application Interchange Profile).

If the current transaction is declined offline and the Combined DDA/AC Generation Failed bit is set to “1” in the TVR received from the terminal, the card sets the Dynamic Data Authentication Failure indicator to “1”.

Processing Restrictions 7

The Processing Restrictions function is performed by the terminal using data elements from the terminal and the card. It includes checks on application versions, effective and expiration dates, and conditions at the point of transaction.

Processing Restrictions shall be performed as specified in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 6.4, and *Book 4*, Section 2.3.3 and Annex A.

This chapter contains the following sections:

7.1 Card Data

7.2 Terminal Data

7.3 Processing

7.4 Prior Related Processing

7.5 Subsequent Related Processing

7.1 Card Data

The card data elements used in Processing Restrictions are listed and described in Table 7–1. For a detailed description of these elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 7–1: Processing Restrictions—Card Data

Data Element	Description
Application Effective Date	The Application Effective Date is the date when the application becomes activated for use.
Application Expiration Date	The Application Expiration Date is the date after which the application is no longer available for use.
Application Version Number	This data element (card tag “9F08”) indicates the version of the application on the card. It is used in Application Version Number checking by the terminal. Cards complying with this specification should use 140.
Application Usage Control (AUC)	The AUC is an optional data element. This data element indicates any restrictions set forth by the issuer on the geographic usage and services permitted for the card application. It is used in Application Usage Control checking by the terminal.
Issuer Country Code	This Issuer Country Code is the EMV-defined data element (tag “5F28”) indicating the country of the card issuance. It is used in Application Usage Control checking by the terminal.

7.2 Terminal Data

The terminal data elements used in Processing Restrictions are listed and described in Table 7–2. For a detailed description of these elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables.

Table 7–2: Processing Restrictions—Terminal Data

Data Element	Description
Application Version Number	This data element (terminal tag “9F09”) indicates the version of the application in the terminal. Terminals complying with this specification should use 140.
Transaction Type	This data element indicates the type of financial transaction. (It is represented by the first two digits of International Organisation for Standardisation (ISO) 8583-1987, Processing Code.) It is used in Application Usage Control checking by the terminal.
Terminal Country Code	This data element indicates the country where the terminal is located. It is used in Application Usage Control checking by the terminal.
Transaction Date	This is the local date (in the terminal) when the transaction is taking place. It is used by the terminal in effective and expiration date checking.

7.3 Processing

The card performs no processing during the Processing Restrictions function.

The following sections describe how the terminal uses data from the card during Processing Restrictions.

7.3.1 Application Version Number

The terminal compares the Application Version Number from the card to the Application Version Number in the terminal to see if they are the same.

7.3.2 Application Usage Control

During Application Usage Control, the terminal checks various conditions at the point of transaction to determine if processing should continue. If the Application Usage Control (AUC) and the Issuer Country Code were received from the card during Read Application Data, the terminal checks the following application restrictions:

1. Domestic and International Checking

   Domestic

   The terminal compares the Issuer Country Code to the Terminal Country Code. If they are equal, the transaction is considered domestic. If the transaction is domestic, the domestic indicator corresponding to Transaction Type must be "1" in the AUC from the card to indicate that the requested service is allowed.

   For example, if the transaction is a cash transaction, the indicator Valid for Domestic Cash Transactions must be "1".

   International

   If the country codes are not equal, the transaction is considered international. If the transaction is international, the international indicator corresponding to Transaction Type must be "1" in the AUC from the card to indicate that the requested service is allowed.

   For example, if the transaction is a cash transaction, the indicator Valid for International Cash Transactions must be "1".

2. ATM Checking

   If the card acceptance device is an ATM, the indicator for "Valid at ATMs" must be "1" in the AUC. If the card acceptance device is not an ATM, the indicator "Valid at terminals other than ATMs" must be "1" in the AUC.

If any of the above checks performed by the terminal fail, the terminal indicates that the "Requested service is not allowed for card product" in the TVR.

The manner in which the AUC from the card is used in this processing is illustrated in Table 7–3. If the indicated bit has a value of "1", that usage or capability is supported.

Table 7–3: Application Usage Control (AUC)

Byte	b8	b7	b6	b5	b4	b3	b2b	b1	Usage
1	1	x	x	x	x	x	x	x	Valid for domestic cash transactions
1	x	1	x	x	x	x	x	x	Valid for international cash transactions
1	x	x	1	x	x	x	x	x	Valid for domestic goods
1	x	x	x	1	x	x	x	x	Valid for international goods
1	x	x	x	x	1	x	x	x	Valid for domestic services
1	x	x	x	x	x	1	x	x	Valid for international services
1	x	x	x	x	x	x	1	x	Valid at ATMs
1	x	x	x	x	x	x	x	1	Valid at terminals other than ATMs
2	1	x	x	x	x	x	x	x	Domestic cashback allowed
2	x	1	x	x	x	x	x	x	International cashback allowed

7.3.3 Application Effective Date

The terminal performs Application Effective Date checking when the card application data includes the Application Effective Date. It ensures that the application is active by validating that the Application Effective Date from the card is less than or equal to the Transaction Date (local to the terminal). If the Application Effective Date is greater than the Transaction Date, the terminal indicates in the TVR that the application is not yet effective.

7.3.4 Application Expiration Date

Application Expiration Date checking is mandatory. The terminal validates that the application has not expired by ensuring that the Application Expiration Date from the card is greater than or equal to the Transaction Date (local to the terminal). If the Application Expiration Date is less than the Transaction Date, the terminal indicates in the TVR that the application has expired.

7.4 Prior Related Processing

Read Application Data

The terminal uses the READ RECORD command to obtain ICC records to be used for the application. These records include the Issuer Country Code, Application Version Number, and Application Expiration Date and, if present, the AUC and Application Effective Date.

7.5 Subsequent Related Processing

Terminal Action Analysis

During Terminal Action Analysis, the terminal checks the Issuer Action Codes (IAC) and Terminal Action Codes (TAC) to determine the transaction disposition if application versions differ, the card is not yet effective or expired, or the requested service is not allowed for the card.

Cardholder Verification 8

Cardholder Verification is used to ensure that the cardholder is legitimate and the card is not lost or stolen.

In Cardholder Verification, the terminal determines the cardholder verification method (CVM) to be used and performs the selected CVM. The results of CVM processing play a role in later processing.

CVMs supported are:

- Offline Plaintext PIN
- Offline Enciphered PIN
- Online PIN
- Signature

Signature may be combined with the offline PIN validation methods. CVM processing is designed to support additional CVMs such as biometric methods as they are adopted. With the offline PIN methods, the validation of the PIN is done within the card. Offline PIN results are included in the online authorization message and should be considered in the issuer's authorization decision.

The terminal uses rules in a CVM List from the card to select the CVM to be used. The selection criteria in the CVM List can include the type of transaction (cash or purchase), the transaction amount, and the CVM capabilities of the terminal. The CVM List also specifies the terminal action if the CVM fails.

Cardholder Verification shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3,* Section 6.5, and *Book 4,* Section 2.3.4.

This chapter is separated into the following sections:

8.1 Card Data

8.2 Terminal Data

8.3 Commands

8.4 Processing

8.5 Prior Related Processing

8.6 Subsequent Related Processing

8.1 Card Data

The terminal uses the data from the card, described in Table 8–1, during CVM List processing. Appendix A, Card and Issuer Data Element Tables, contains detailed descriptions of the card data elements and their usage.

Table 8–1: CVM List Processing—Card Data (1 of 2)

Data Element	Description
Application Currency Code	Used to determine whether the transaction is in the card's currency. If the CVM List is present and the value for either Amount X or Amount Y in the CMV List is not zero, Application Currency Code shall be present.
Application Interchange Profile (AIP)	Contains an indicator showing whether the card supports cardholder verification. This indicator shall be set to "1".

Table 8–1: CVM List Processing—Card Data (2 of 2)

Data Element	Description
Cardholder Verification Method (CVM) List	Identifies a prioritized list of methods of cardholder verification for the card application. A card shall contain a CVM List and may contain multiple CVM Lists for use in different types of transactions such as international and domestic transactions. A CVM List contains the following: • Amount X—Amount used in CVM usage conditions • Amount Y—Second amount used in CVM usage conditions • CVM entries—The CVM List may contain multiple entries. Each entry contains the following subfields: **Subfield** — **Description** CVM Code — Designates the action to take if the CVM fails. Choices are to process the next CVM entry or to fail CVM processing. CVM Type — The type of CVM to perform: • Plaintext PIN verified offline • Enciphered PIN verified online • Plaintext PIN verified offline and signature • Signature • Enciphered PIN verified offline • Enciphered PIN verified offline and signature • No CVM required (CVM is considered to have passed with no other CVM processing) • Fail CVM processing (CVM processing is considered to have failed with no other CVM processing) CVM Conditions — Conditions when this CVM entry should be used: • Always • If transaction is cash or cashback • If transaction is not cash or cashback • If the terminal supports the CVM • If transaction amount is less than Amount X • If transaction amount is more than Amount X • If transaction amount is less than Amount Y • If transaction amount is more than Amount Y ***Note:*** *The last four conditions require that the transaction be in the card's Application Currency.*

The following is an example of how an issuer might define a CVM List:

EXAMPLE

CVM List

An issuer wishes to verify cardholders in the following manner:

- Online PIN for all ATM transactions and cashback transactions
- Offline PIN for point-of-service (POS) transactions if the terminal supports Offline PIN
- Signature for POS transactions if the terminal does not support Offline PIN
- No signature is required for POS transactions if the terminal does not support signature or Offline PIN

The CVM List shown in Table 8–2 could be used.

Table 8–2: Sample CVM List

Entry	Value/Meaning	Comments
Amount X	0	No amount checks in CVM List
Amount Y	0	No amount checks in CVM List
CVM Entry 1		ATM transactions use this CVM List entry.
CVM Condition	01/If cash or cashback	
CVM Type	000000b/Enciphered PIN verified online	
CVM Code	1b/Fail cardholder verification if CVM fails	
CVM Entry 2		POS transactions get to here. Use this CVM if terminal supports Offline Plaintext PIN.
CVM Condition	03/If terminal supports CVM	
CVM Type	000001b/Offline Plaintext PIN	
CVM Code	1b/Fail cardholder verification if CVM fails	
CVM Entry 3		Get to here if terminal does not support Offline Plaintext PIN. Use this CVM if the terminal supports signature collection.
CVM Condition	03/If terminal supports CVM	
CVM Type	011110b/Signature	
CVM Code	0b/Go to next CVM if CVM fails	
CVM Entry 4		Get to here if terminal does not support signature or Offline PIN. CVM will never fail.
CVM Condition	00/Always	
CVM Type	011111b/No CVM Required	
CVM Code	1b/Fail cardholder verification if CVM fails	

The card uses the card data, described in Table 8–3, for Offline PIN Processing.

Table 8–3: Offline PIN Processing—Card Data

Data Element	Description
PIN Try Limit	Issuer-specified maximum number of consecutive incorrect PIN tries allowed
PIN Try Counter	Designates the number of PIN tries remaining. If supported, the card returns the PIN Try Counter in the GET DATA response. It is put in the VERIFY response to notify the terminal whether additional PIN entry attempts are permitted. The PIN Try Counter shall be present if the card supports offline PIN verification. The card shall decrement the PIN Try Counter with each unsuccessful VERIFY command received from the terminal and shall reset it to the PIN Try Limit when the Transaction PIN matches the Reference PIN or when a script command to reset the counter is processed. It is not necessary that the PIN Try Counter be retrievable by the terminal. An issuer should choose to have the PIN Try Counter retrievable using the GET DATA command if the issuer wishes the “Last PIN Try” message to be displayed prior to PIN entry when a card with one remaining PIN try is used at a terminal or if the terminal should not request PIN entry when the PIN Try Limit is exceeded. Otherwise, the PIN Try Counter shall be a Visa proprietary data element that is not accessible by the terminal using GET DATA.
Reference PIN	The cardholder PIN which the card compares to the Transaction (key-entered) PIN during offline PIN processing. The Reference PIN shall be present if the card supports offline PIN verification. The Reference PIN shall be stored securely within the card in one or more proprietary internal files. It shall be backed up. The Reference PIN shall never be retrievable by a terminal or any outside source and shall never be updated with the following exception: If the issuer supports changing the Reference PIN through Issuer Script processing, the Reference PIN may be updated if an Issuer Script Command such as the PIN CHANGE/UNBLOCK command is successfully performed during Issuer Script processing with secure messaging. Chapter 14 describes Issuer Script processing.
Card Verification Results (CVR)	Contains indicators that the card sets for the following CVM conditions: • Offline PIN Verification Performed • Offline PIN Verification Failed • PIN Try Limit Exceeded • Application Blocked because PIN Try Limit Exceeded

Cards supporting Offline Enciphered PIN shall either use an ICC PIN Encipherment public/private key pair or shall use the ICC public/private key pair used for DDA. Chapter 6, Offline Data Authentication, provides additional detail on generating and using the RSA public/private key data elements required for Offline Enciphered PIN which are described in Table 8–4.

Table 8–4: Offline Enciphered PIN Processing—Card Data

Data Element	Description
ICC PIN Encipherment or ICC Public Key (PK) Certificate	Signed with the Issuer Private Key. Contains the public key to be used to encipher the PIN for Offline Enciphered PIN. The format of the ICC PIN Encipherment PK Certificate is shown in the *EMV 4.0, Book 2*, Table 19.
ICC PIN Encipherment or ICC Public Key Remainder	Contains the portion, if necessary, of the public key that does not fit into the ICC's public key certificate.
ICC PIN Encipherment or ICC Public Key Exponent	Contains the exponent used in the algorithm that enciphers the PIN for Offline Enciphered PIN. Shall be 3 or $2^{16} + 1$.
ICC PIN Encipherment or ICC Private Key	Stored in a secret, secure location on the card and never passed to the terminal. Used to decipher the enciphered PIN passed to the card in the VERIFY command during Offline Enciphered PIN.
Issuer Public Key (PK) Certificate	Signed with the Visa Private Key. Contains the public key to be used to decipher the ICC PIN Encipherment or ICC PK Certificate.
Issuer Public Key Remainder	Contains the portion, if necessary, of the Issuer Public Key that does not fit into the Issuer PK Certificate.
Issuer Public Key Exponent	Contains the exponent used in the algorithm that deciphers the ICC PIN Encipherment or ICC PK Certificate.Shall be 3 or $2^{16} + 1$.
Certificate Authority Public Key Index (PKI)	Used with the Registered Application Provider Identifier (RID) to identify which Visa Private Key was used to encrypt the Issuer PK Certificate and which corresponding Visa Public Key must be used to recover the Issuer PK Certificate.
Issuer Public Key Data	Used to decipher the ICC PIN Encipherment or ICC PK Certificate. This is the same certificate and other Issuer Public Key data used for DDA and SDA (see Chapter 6, Offline Data Authentication).
Registered Application Provider Identifier (RID)	The part of the Application Identifier (AID that identifies the Application Provider (scheme). The RID and the PKI are used to identify the Visa Public Key to be used to recover the Issuer PK Certificate.

8.2 Terminal Data

The terminal uses the terminal data, described in Table 8–5, during PIN processing. The *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables, contains detailed descriptions of the terminal data elements and their usage.

Table 8–5: PIN Processing—Terminal Data

Data Element	Description
Transaction PIN	Data entered by the cardholder for the purpose of PIN verification.

8.3 Commands

The following commands are used for offline PIN processing:

- **GET DATA**—Used by the terminal to obtain the PIN Try Counter from the card in order to determine whether the PIN Try Limit was exceeded on a previous transaction or is close to being exceeded. Support for accessing the PIN Try Counter using GET DATA is optional.

  If the card does not support accessing the PIN Try Counter with the GET DATA command, SW1 SW2 in the command response shall not be "9000" ("6A88" is recommended.)

- **GET CHALLENGE**—The GET CHALLENGE command is used to obtain an unpredictable number from the card for use in Offline Enciphered PIN processing.

  The card shall support the GET CHALLENGE command if the card supports Offline Enciphered PIN processing.

- **VERIFY**—Used for Offline Enciphered PIN and Offline Plaintext PIN. The VERIFY command initiates the card comparison of the cardholder-entered Transaction PIN with the Reference PIN.

  The card shall support the VERIFY command if the card supports Offline PIN processing.

  The P2 parameter indicates whether the Transaction PIN is plaintext or enciphered:

  – "80" if the PIN is plaintext

  – "88" if the PIN is enciphered

SW1 SW2 in the command response shall be set to the following:

– "9000" if the Transaction PIN matches the Reference PIN.

– "63Cx" if the PINs do not match. The "x" value represents the number of PIN tries remaining.

– "6984" when initial use of the VERIFY command shows the PIN Try Limit was exceeded on a previous transaction.

– "6983" when a subsequent VERIFY command is received by the card after the PIN Try Limit has been exceeded during the current transaction.

8.4 Processing

The following describes the card's role in processing the CVM List and the various CVMs.

8.4.1 CVM List Processing

Other than supplying the CVM List during Read Application Data, the card plays no role in CVM List processing.

8.4.2 Offline PIN Processing

The following requirements apply whether a PIN is transmitted in the clear to the card or the PIN is enciphered at the PIN pad or card reader and deciphered by the card.

1. Checking the PIN Try Counter

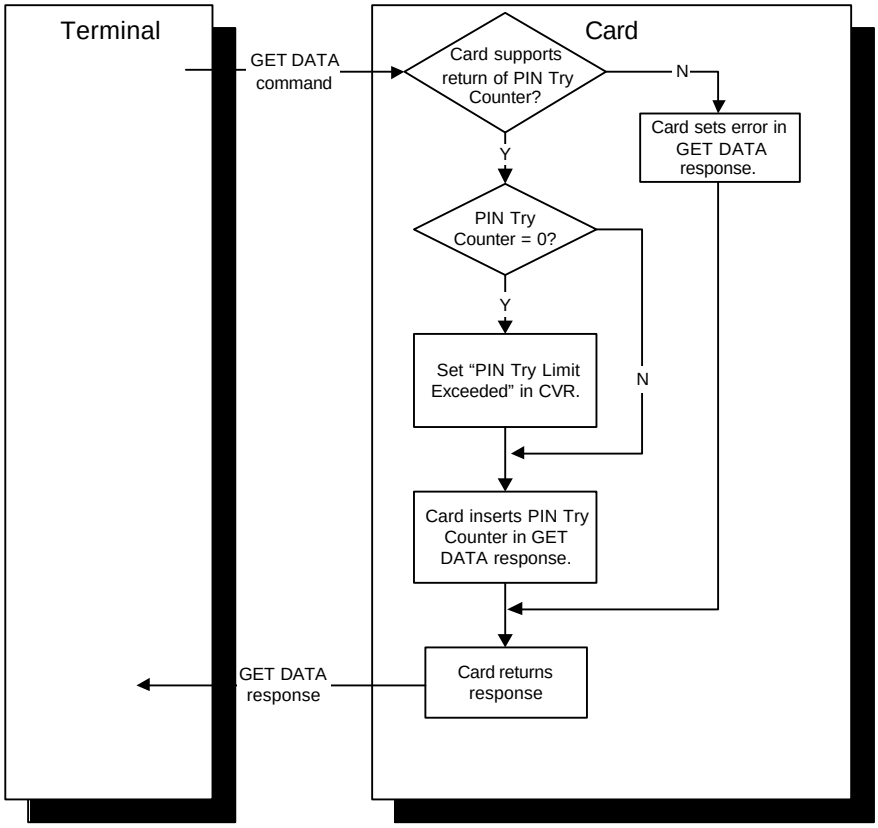
   After the terminal determines that an offline PIN is to be entered, the terminal may transmit a GET DATA command to the card to retrieve the PIN Try Counter.

   a. If the card supports returning the PIN Try Counter with the GET DATA command, the card shall:

      - Set the PIN Try Limit Exceeded bit to "1" in the CVR if the PIN Try Counter is zero.
      - Return the PIN Try Counter to the terminal in the GET DATA response. The terminal does not allow offline PIN entry if the PIN Try Counter is zero.

   b. If the card does not support return of the PIN Try Counter with the GET DATA command, the card shall return an SW1 SW2 error code to the terminal. This error code should be "6A88".

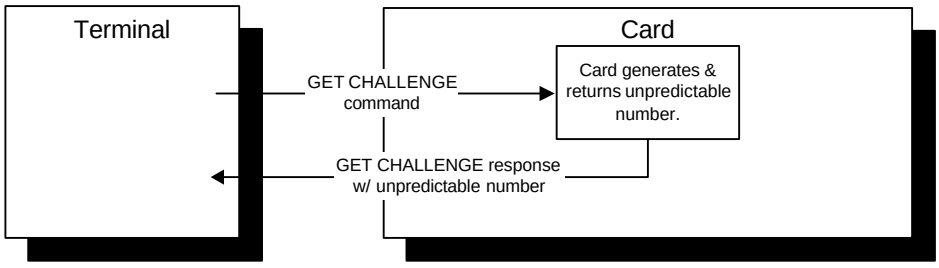
Figure 8–1: Checking The PIN Try Counter



2. PIN Encipherment

   If the CVM is Offline Enciphered PIN, the terminal requests an unpredictable number from the card using the GET CHALLENGE command. The card shall generate and return an unpredictable number that the terminal uses in the PIN encipherment algorithm.

Figure 8–2: PIN Encipherment



3. Receiving the VERIFY command

   After the Transaction PIN is entered, the terminal transmits a VERIFY command containing this PIN. When the VERIFY command is received, the card shall set Offline PIN Verification Performed to "1" in the CVR.

   The Transaction PIN may be plaintext or enciphered as shown by the P2 parameter of the VERIFY command:

   a. P2 = "80"—The PIN is in the clear. The card shall proceed to the PIN Verification step.

   b. P2 = "88"—The PIN is enciphered. The card shall decipher the PIN using the ICC PIN Encipherment Private Key, if present, or ICC Private Key if the ICC PIN Encipherment Private Key is not present. This process is described in the *EMV 4.0, Book 2*, Section 7. If errors occur during PIN decipherment, PIN verification has failed.

4. PIN Verification

   The card performs the following PIN verification steps:

   a. PIN Try Limit Already Exceeded

      If the PIN try function is blocked because the PIN Try Limit was exceeded previously, the card shall:

      - Set the CVR PIN Try Limit Exceeded to "1"
      - Set the CVR Offline PIN Verification Failed bit to "1"
      - Return SW1 SW2 = "6984" in the VERIFY response if the PIN Try Limit was exceeded on a previous transaction
      - Return SW1 SW2 = "6983" in the VERIFY response if the PIN Try Limit was exceeded during the current transaction

   b. Matching PINs

      If the PIN try function is not blocked, the card shall compare the Transaction PIN to the Reference PIN. If they match, the card shall:

      - Reset the PIN Try Counter to the PIN Try Limit value
      - Set the CVR Offline PIN Verification Failed bit to "0"
      - Return a VERIFY command response indicating that the command was successfully executed (SW1 SW2 = "9000").

c. Non-Matching PINs

If the Transaction PIN does not match the Reference PIN, the card shall:

- Decrement the PIN Try Counter by one
- Set the CVR Offline PIN Verification Failed bit to “1”

The card shall determine whether the PIN Try Limit was exceeded:

- No PIN tries remaining

  If the resulting value of the PIN Try Counter is zero, the card shall

  – Set the CVR PIN Try Limit Exceeded bit to “1”

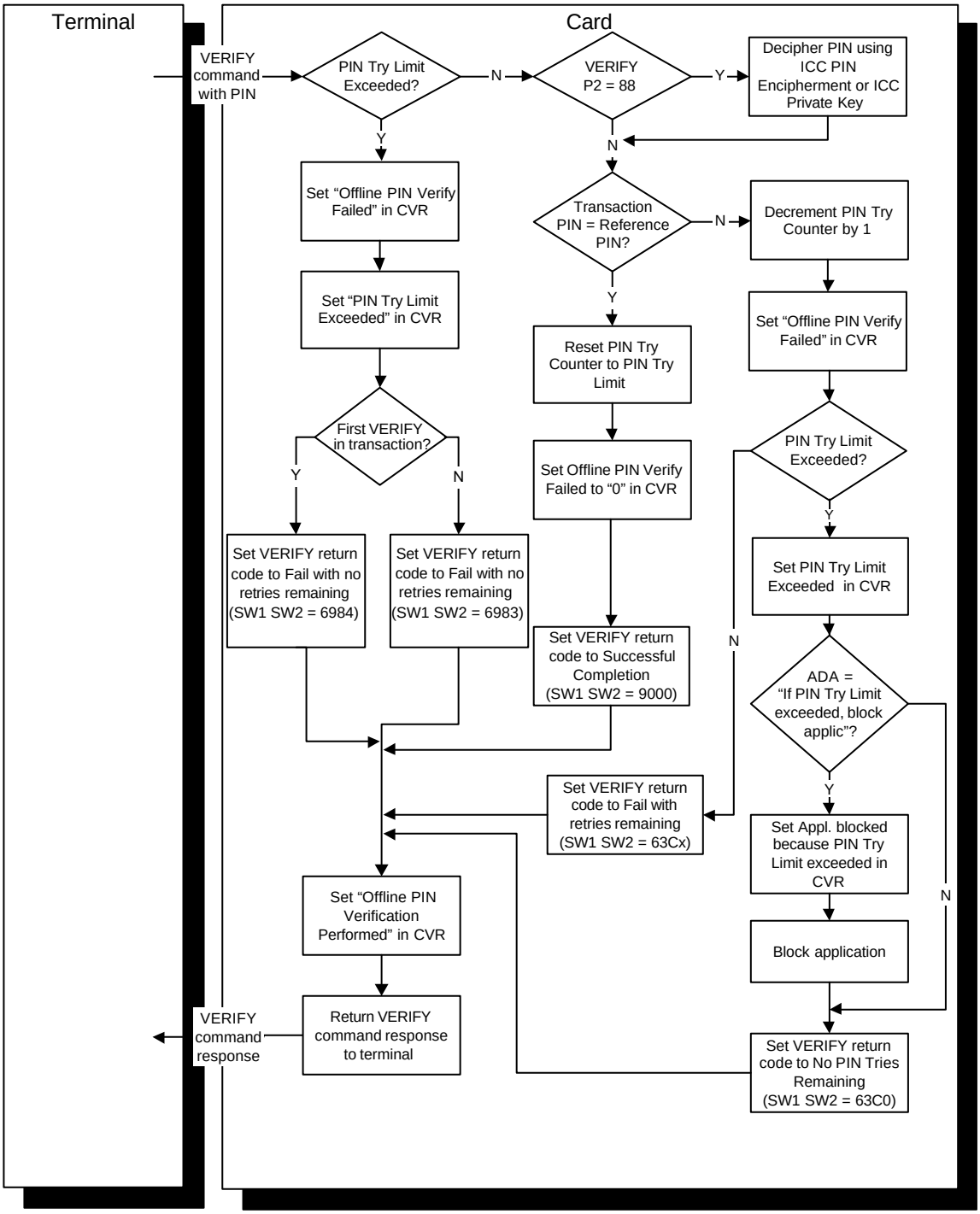
  – If Application Default Action (ADA) is present and PIN Try Limit Exceeded on Current Transaction, Block Application bit in the ADA is “1”, set the Application Blocked by Card because PIN Try Limit Exceeded bit to “1” in the CVR and block the application. The card shall allow the current transaction to proceed through Completion. Blocking the application as described here shall not permanently disable the application or the card.

  – Return a VERIFY command response indicating that the PIN Try Limit is exceeded (SW1 SW2 = “63C0”)

- PIN Tries Remaining

  If the resulting value of the PIN Try Counter is not zero, the card shall return a VERIFY command response indicating the remaining number of PIN tries (SW1 SW2 = “63Cx” where x equals the remaining PIN tries).

Figure 8–3: Offline PIN Processing



5. Follow-up Processing

   After each unsuccessful PIN try with PIN tries remaining, the terminal requests another PIN entry and sends the card another VERIFY command.

   If PIN verification is successful prior to the PIN Try Counter being decremented to zero, the card shall:

   – Reset the PIN Try Counter to the value of the PIN Try Limit

   – Set the Offline PIN Verification Failed bit to "0" in the CVR.

   The cardholder may continue to enter a PIN until the PIN Try Counter is decremented to zero. At that time, the terminal will not transmit any further VERIFY command messages to the card.

8.4.3 Processing of Other CVMs

The card plays no role in the processing of Online PIN or signature.

8.5 Prior Related Processing

Initiate Application Processing

The terminal receives the Application Interchange Profile (AIP) which indicates whether the card supports cardholder verification in the GET PROCESSING OPTIONS response from the card.

Read Application Data

The terminal reads the CVM List and other data used in CVM processing from the card.

8.6 Subsequent Related Processing

Terminal Action Analysis

The terminal uses cardholder verification results and card and terminal parameters to determine whether the transaction should be declined offline, sent online, or approved online.

Card Action Analysis

The card uses parameters in ADA to determine whether to create an advice when the PIN Try Limit is exceeded.

The card uses ADA parameters to determine whether to decline or send a transaction online if the PIN Try Limit was exceeded on one of the card's previous transactions.

Online Processing

CVM results including Offline PIN results are included in the authorization request and should be considered in the Issuer's authorization decision.

If the CVM is Online PIN, the enciphered PIN is included in the online request. If the CVM is Offline PIN, the PIN is not included in the online authorization request.

Completion

If the terminal attempted to go online for an authorization for a transaction where the PIN Try Limit is exceeded and this attempt failed, the card uses parameters in ADA to determine whether to decline the transaction.

Issuer-to-Card Script Processing

The PIN CHANGE/UNBLOCK command can be used to reset the PIN Try Counter to equal the PIN Try Limit and to change the Reference PIN.

The APPLICATION UNBLOCK command can be used to unblock an application which was blocked during CVM processing.

Terminal Risk Management 9

Terminal Risk Management provides issuer authorization for higher-value transactions and ensures that chip-read transactions initiated from cards go online periodically to protect against credit and fraud risks that might be undetectable in an offline environment.

Issuers are required to support Terminal Risk Management. Terminals are required to perform Terminal Risk Management for Visa transactions whether or not it is supported by the card.

Terminal Risk Management shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 6.6, and *Book 4*, Section 2.3.5.

This chapter is organized as follows:

9.1 Card Data

9.2 Terminal Data

9.3 GET DATA Command

9.4 Processing

9.5 Prior Related Processing

9.6 Subsequent Related Processing

9.1 Card Data

The card data elements used by the terminal in Terminal Risk Management are listed and described in Table 9–1. For a detailed description of these elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 9–1: Terminal Risk Management—Card Data

Data Element	Description
Application Primary Account Number (PAN)	The cardholder account number for the application
Application Transaction Counter (ATC)	A counter of transactions initiated since the application was put on the card. Maintained by the application on the card.
Last Online Application Transaction (ATC) Register	ATC value of the last online authorization where Issuer Authentication requirements were satisfied. If the card mandates Issuer Authentication, the register is reset to the value of the ATC during Completion when Issuer Authentication is performed and passes. If Issuer Authentication is optional or not supported, it is reset whenever an online authorization is completed and Issuer Authentication does not fail. Used in terminal velocity checking and new card checking.
Lower Consecutive Offline Limit “9F14”	The Issuer-specified limit for the number of consecutive offline transactions allowed before a transaction must be sent online if the terminal is online capable. It is used in terminal velocity checking and required for terminal new card checking.
Upper Consecutive Offline Limit “9F23”	The Issuer-specified limit for the number of consecutive offline transactions allowed before transactions must be sent online. If an online authorization cannot be completed, the transaction is declined offline. It is used in terminal velocity checking and required for terminal new card checking.

9.2 Terminal Data

The terminal data elements used in Terminal Risk Management are listed and described in Table 9–2. For a detailed description of these elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables.

Table 9–2: Terminal Risk Management—Terminal Data

Data Element	Description
Amount, Authorized	This numeric data element (tag “9F02”) stores the amount (excluding adjustments) for the current transaction. It is used in floor limit checking.
Maximum Target Percentage to be used for Biased Random Selection	Value used for random selection of transactions for online processing.
Target Percentage to be used for Random Selection	Value used for random selection of transactions for online processing.
Terminal Floor Limit	Indicates the floor limit in the terminal for the application. It is used in floor limit checking and random selection of transactions for online processing.
Terminal Verification Results (TVR)	A series of indicators in which the results of offline processing from a terminal perspective are recorded. It is used to record the results of all terminal risk management checks.
Threshold Value for Biased Random selection	Value used for random selection of transactions for online processing.
Transaction Log	To prevent the use of split sales to bypass floor limits, the terminal may maintain a transaction log of approved transactions. This log, minimally contains the Application PAN and transaction amount, and optionally contains the Application PAN Sequence Number and Transaction Date. The number of transactions to be stored and maintenance of the log are outside the scope of this specification. This log, if present, may be used in terminal floor limit checking.
Transaction Status Information (TSI)	Indicates the functions performed by the terminal. This data element is not provided in the online authorization and clearing messages, but is used by the terminal to indicate that Terminal Risk Management was performed.

9.3 GET DATA Command

The terminal issues GET DATA commands to request the Last Online ATC Register and the Application Transaction Counter (ATC) from the card, if not already present in the terminal. These data elements are used in terminal velocity checking and the new card checks.

If the card supports terminal velocity checking or the new card check done by the terminal, it shall return these data elements to the terminal in the command response.

If the card does not support terminal velocity checking or a terminal new card check, these data elements shall be stored as Visa proprietary data elements and shall not be returned to the terminal. The card should return SW1 SW2 = “6A88” when the data is not accessible.

9.4 Processing

Except for responding to the GET DATA command during Terminal Velocity Checking and the New Card check, the card does no processing during Terminal Risk Management.

The following describes how the terminal uses data from the card during the Terminal Risk Management processes:

9.4.1 Terminal Exception File

If a terminal exception file is present, the terminal checks whether the Application Primary Account Number (PAN) from the card is listed on the exception file.

9.4.2 Merchant Forced Transaction Online

At online-capable terminals, the merchant may indicate to the terminal that the transaction should be processed online. No card data is used in this process.

9.4.3 Floor Limits

Floor limit checking is performed so that transactions with amounts above the Terminal Floor Limit are sent online for authorization. No card data is used in this process.

9.4.4 Random Transaction Selection

Terminals capable of supporting both offline and online transactions shall randomly select transactions for online processing. No card data is used in this process.

9.4.5 Terminal Velocity Checking

Velocity checking permits issuers to request online processing after a specified number of consecutive offline transactions. Issuers may elect not to support velocity checking by the terminal by not personalizing the Upper and Lower Consecutive Offline Limits (tags “9F14” and “9F23” respectively) on the card.

During velocity checking, the terminal issues the GET DATA command to request the Last Online ATC Register and the ATC.

The card responds to the GET DATA command with the Last Online ATC Register and the ATC if these data elements are accessible using GET DATA.

The number of consecutive offline transactions is the difference between the ATC and the Last Online ATC Register.

NOTE: *The card may perform similar velocity checks during Card Action Analysis.*

9.4.6 New Card Check

In new card checking by the terminal, the terminal checks whether the Last Online ATC Register, if available from the card, is zero.

The terminal issues the GET DATA command to request the Last Online ATC Register if it was not received during Terminal Velocity Checking. The card responds with the Last Online ATC Register if the register is not stored as a Visa proprietary data element.

NOTE: *The card may perform a similar new card check during Card Action Analysis.*

9.5 Prior Related Processing

Read Application Data

The following data is read from the card:

- Application Primary Account Number (PAN) used in checking the terminal exception file.
- Upper and Lower Consecutive Limits used in Terminal Velocity Checking, if present on the card.

9.6 Subsequent Related Processing

Terminal Action Analysis

Based on card and terminal settings, the terminal determines what action to take if:

- Card was on terminal exception file
- Merchant forced transaction online
- Floor Limits were exceeded
- Transaction was randomly selected for online processing
- Velocity Checking amounts or counters were exceeded
- Card was a new card

Terminal Action Analysis 10

In Terminal Action Analysis, the terminal applies rules set by the issuer in the card and by the payment system in the terminal to the results of offline processing to determine whether the transaction should be approved offline, declined offline, or sent online for an authorization. Terminal Action Analysis involves two steps:

1. **Review Offline Processing Results**—The terminal reviews the results of offline processing to determine whether the transaction should go online, be approved offline, or be declined offline. This process considers issuer-defined criteria from the card called Issuer Action Codes (IACs) and Visa-defined criteria in the terminal called Terminal Action Codes (TACs).
2. **Request Cryptogram**—The terminal requests a cryptogram from the card.

A decision for an offline approval or to go online made during Terminal Action Analysis is not final. As a result of Card Action Analysis (see Chapter 11, Card Action Analysis), the card may override the terminal's decision. Decisions to decline offline may not be overridden.

Terminal Action Analysis shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 6.7, and *Book 4*, Section 2.3.6.

This chapter is organized into the following sections:

10.1 Card Data
10.2 Terminal Data
10.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command
10.4 Processing
10.5 Prior Related Processing
10.6 Subsequent Related Processing

10.1 Card Data

The terminal uses the card data elements described in Table 10–1 in Terminal Action Analysis. For a detailed description of card data elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 10–1: Terminal Action Analysis—Card Data

Data Element	Description
Issuer Action Codes (IACs)	The IACs are three data elements, each consisting of a series of bits corresponding to the bits in the Terminal Verification Results (TVR). During personalization, the issuer should set an IAC bit to “1” if the corresponding TVR condition is to result in the action designated by the IAC. The three IACs are: • IAC—Denial The issuer sets the IAC bits to “1” that correspond to the TVR bits for conditions which the issuer wishes to result in an offline decline. • IAC—Online The issuer sets the bits to “1” that correspond to the TVR bits for conditions which the issuer would like to result in an online authorization. • IAC—Default The issuer sets the bits to “1” that correspond to the TVR bits for conditions which the issuer would like to default to an offline decline if online processing is requested but not available.

The Terminal Volume, Chapter 10, Terminal Action Analysis, contains an example of how the IACs and TACs are used with the Terminal Verification Results (TVR) to determine transaction disposition.

The IACs are included in the data elements recommended for validation by Offline Data Authentication. If the IACs are included in the validation data, they should not be changed without also updating the Signed Static Application Data (SAD) and the ICC PK Certificate. Otherwise, SDA and DDA will fail.

The card data elements described in Table 10–2 were previously received from the card and are used during Request Cryptogram Processing.

Table 10–2: Request Cryptogram Processing—Card Data

Data Element	Description
Card Risk Management Data Object List 1 (CDOL1)	The CDOL1 shall contain the tags and lengths for the terminal data objects that are needed by the card to generate an application cryptogram or for other card processing. Refer to Appendix E, Cryptogram Versions Supported, for cryptogram CDOL1 requirements. Chapter 11, Card Action Analysis, shows the CDOL1 requirements for Card Action Analysis. The TC Hash Value is included in the CDOL1 if the cryptogram algorithm uses pre-hashing.
Transaction Certificate Data Object List (TDOL)	Optional list of data objects (tags and lengths) used by the terminal in generating the optional TC Hash Value. The cryptogram versions defined in Appendix E, Cryptogram Versions Supported, do not use the TDOL. Rules for use of the TDOL are in the *EMV 4.0, Book 3*, Section 5.2.2.

10.2 Terminal Data

The terminal uses the terminal data elements described in Table 10–3 in Terminal Action Analysis. For a detailed description of these data elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables.

Table 10–3: Review Offline Processing Results—Terminal Data

Data Element	Description
Terminal Action Codes (TACs)	The TACs are three data elements each consisting of a series of bits corresponding to the bits in the Terminal Verification Results (TVR). Similar to card's IACs, the TAC bits are set to "1" if the corresponding TVR bit is to result in the action specified by the TAC. These actions are decline offline, go online for an authorization, and decline offline if the online authorization is unable to complete. The Visa-required TAC values are listed in Chapter 10 of the Terminal volume.

The terminal uses the terminal data elements described in Table 10–4 when requesting cryptogram processing.

Table 10–4: Request Cryptogram Processing—Terminal Data

Data Element	Description
Terminal Data Elements	The terminal data elements specified in the CDOL1 or TDOL from the card are included in the GENERATE AC command.
TC Hash Value	Optional hash calculated by the terminal which may be used as input to the GENERATE AC command. The formatting and calculation of the TC Hash Value is described in Appendix D, Authentication Keys and Algorithms. The cryptogram versions described in Appendix E, Cryptogram Versions Supported, do not use a TC Hash Value.

10.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command

The terminal uses the GENERATE APPLICATION CRYPTOGRAM (AC) command to request a Triple DES application cryptogram from the card.

The P1 parameter of the command indicates the cryptogram type being requested and whether the cryptogram is eligible for Combined DDA/AC Generation. The *EMV 4.0, Book 3*, Table I-12, shows the coding of this parameter. The data portion of the command contains the terminal data objects requested in the CDOL1. The CDOL1 was received from the card during Read Application Data. Eligibility for Combined DDA/AC Generation is also indicated when the CDOL1 contains the tag for Terminal Capabilities and the Terminal Capabilities from the terminal and the card's Application Interchange Profile indicate that both support Combined DDA/AC Generation.

The card processes the GENERATE AC command and returns the command response during Card Action Analysis (Chapter 11, Card Action Analysis).

10.4 Processing

10.4.1 Review Offline Processing Results

The Review Offline Processing Results step of Terminal Action Analysis is performed entirely within the terminal using processing rules called IACs that were received from the card earlier in the transaction and payment scheme rules from the terminal called TACs.

The card performs no processing during the Review Offline Processing step.

10.4.2 Request Cryptogram Processing

In the Request Cryptogram Processing step of Terminal Action Analysis, the terminal sends a GENERATE AC command to the card requesting generation of an application cryptogram. The command includes the data specified in the CDOL1.

When the card receives the GENERATE AC command, it proceeds to Card Action Analysis (Chapter 11, Card Action Analysis).

10.5 Prior Related Processing

Read Application Data

During Read Application Data, the card sends application data records to the terminal. These data records include the IACs and the CDOL1 that are used during Terminal Action Analysis.

10.6 Subsequent Related Processing

Card Action Analysis

During Card Action Analysis, the card performs additional risk management to determine whether it agrees with the terminal's Terminal Action Analysis decision to approve offline, decline offline, or send online.

Card Action Analysis 11

Card Action Analysis allows issuers to perform velocity checking and other risk management checks that are internal to the card. Visa proprietary Card Risk Management features described in this section include checking:

- Activity on previous transactions
- If card is a new card
- Offline transaction counters and amount accumulators

After completing Card Risk Management, the card returns an Application Cryptogram to the terminal. This cryptogram is an AAC for an offline decline, an ARQC for a request for an online authorization, and a TC for an offline approval. If supported by both the card and terminal, the terminal may request Combined DDA/AC Generation where the card returns an ARQC or TC as part of a dynamic signature.

Card Action Analysis shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 6.8.

This chapter is organized as follows:

11.1 Card Data

11.2 Terminal Data

11.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command

11.4 Processing

11.5 Card Provides Response Cryptogram

11.6 Processing Flow

11.7 Prior Related Processing

11.8 Subsequent Related Processing

11.1 Card Data

The card data elements used in Card Action Analysis are listed and described in Table 11–1. For a detailed description of these elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 11–1: Card Action Analysis—Card Data (1 of 4)

Data Element	Description
Application Cryptogram	A cryptogram returned by the card in the response to the GENERATE APPLICATION CRYPTOGRAM (AC) command. • An Application Authentication Cryptogram (AAC) for offline declines. • A Transaction Certificate (TC) for offline approvals. • An Authorization Request Cryptogram (ARQC) when online processing is requested.
Application Currency Code	A code indicating the domestic currency associated with the application.
Application Default Action (ADA)	Contains Issuer-specific indicators for the card action for exception conditions. If not present, the value defaults to zeros.
Application Interchange Profile (AIP)	Contains indicators showing the capability of the card to support Combined DDA/AC Generation and Issuer Authentication
Card Risk Management Data Object List 1 (CDOL1)	List of data objects (tags and lengths) to be passed to the card application with the first GENERATE AC command. The tags for the following data elements should be present in the CDOL1 for the listed Card Risk Management checks to occur: • Transaction Currency Code—Velocity Checking for Total Consecutive Offline International transactions (Based on Currency), Velocity Check for Total Transaction Amount in Designated Currency, and Velocity Check for Total Transaction Amount (Dual Currency) • Terminal Country Code—Velocity Checking for Total Consecutive International Transactions (Based on Country) • Amount, Authorized—Velocity Checking for Total Transaction Amount in Designated Currency and Velocity Checking for Transaction Amount (Dual Currency) • Terminal Verification Results (TVR)—Contains indicators showing SDA and DDA failure Tags for any of these data elements that are already included in the CDOL1 as part of the data used for cryptogram generation should not be repeated.

Table 11–1: Card Action Analysis—Card Data (2 of 4)

Data Element	Description
Card Verification Results (CVR)	Visa proprietary data element indicating the results of offline processing from current and previous transactions from a card perspective. This data is transmitted online as part of the Issuer Application Data.
Cryptogram Information Data (CID)	Returned to the terminal in the GENERATE AC response. The CID designates the type of cryptogram that is being returned. The CID also includes an additional indicator for advice required and a reason code for the advice or a referral.
Consecutive Transaction Counter (International)	A Visa proprietary counter that is incremented for each offline transaction which is not in the card's designated currency.
Consecutive Transaction Limit (International)	The number of offline international transactions allowed (where the transactions are in a currency other than the card's designated currency) before online processing is requested.
Consecutive Transaction Counter (International—Country)	Visa proprietary counter that is incremented for each offline transaction where the Issuer Country Code differs from the Terminal Country Code.
Consecutive Transaction Limit (International—Country)	Visa proprietary data element specifying the number of offline international transactions allowed (where the Issuer Country Code differs from the Terminal Country Code) before online processing is requested.
Cumulative Total Transaction Amount	Visa proprietary data element specifying the cumulative amount of offline approved transactions in the designated currency (Application Currency Code) since the last online transaction.
Cumulative Total Transaction Amount Limit	Visa proprietary data element specifying the limit on the total amount of offline approved domestic transactions in the designated currency (Application Currency Code) since the last online transaction. If exceeded, online processing is requested.
Cumulative Total Transaction Amount (Dual Currency)	Visa proprietary data element specifying the amount of offline approved transactions in the designated currency (Application Currency Code) or the secondary currency converted to the designated currency since the last online transaction.
Cumulative Total Transaction Amount Limit (Dual Currency)	Visa proprietary data element specifying the limit on the cumulative total amount of offline approved transactions in the designated currency (Application Currency Code) plus a secondary currency (converted to the designated currency) since the last online transaction. If exceeded, online processing is requested.

Table 11–1: Card Action Analysis—Card Data (3 of 4)

Data Element	Description
Currency Conversion Factor	A decimal value used in the dual currency algorithm to convert the value of the amount designated in the Secondary Application Currency to the card's domestic currency (designated by the Application Currency Code). This converted value is used for comparisons only. The Amount, Authorized remains in the Transaction Currency. This field is 4 bytes with the first nibble representing the number of positions the decimal separator in the conversion factor shall be shifted from the right to obtain the actual factor. The following 7 nibbles are the conversion factor. This rate is an approximation and should be limited to two significant digits. The Currency Conversion Factor may be updated using an Issuer Script command. Because this rate is intended to be an approximation, update should not be necessary for minor currency fluctuations.
Dynamic Data Authentication Failure Indicator	An internal application indicator that is set when DDA has failed on a previous transaction and the transaction was declined offline.
Issuer Authentication Failure Indicator	An internal application indicator that is set when one of the following Issuer Authentication error conditions occurred on the last online transaction: • Issuer Authentication performed and failed • Issuer Authentication is mandatory and was not performed
Issuer Authentication Indicator	An indicator designating Issuer Authentication as mandatory or optional when Issuer Authentication is supported.
Issuer Country Code (“9F57”)	A Visa Proprietary data element indicating the country of issuance
Issuer Script Command Counter	An internal application counter that indicates the number of Issuer Script commands requiring secure messaging processed on the last online transaction.
Issuer Script Failure Indicator	An internal application indicator that is set when Issuer Script processing failed on the last online transaction.
Lower Consecutive Offline Limit “9F58”	Visa proprietary data element indicating the maximum number of consecutive offline transactions allowed before an online authorization is requested.
Offline Decline Requested by Card Indicator	An internal application indicator that is set when Card Risk Management checks indicate that a transaction should be declined offline
Online Authorization Indicator	An internal application indicator that indicates that an online transaction was unable to go online or was interrupted prior to completion of the online authorization.

Table 11–1: Card Action Analysis—Card Data (4 of 4)

Data Element	Description
Online Requested by Card Indicator	An internal application indicator that is set when Card Risk Management checks indicate that a transaction should be sent online for processing.
PIN Try Counter	Number of PIN tries remaining.
Secondary Application Currency Code	A code indicating a secondary currency to be converted to the domestic currency for dual currency velocity checking.
Static Data Authentication Failure Indicator	An internal application indicator that is set when SDA has failed on a previous transaction and the transaction was declined offline.

11.2 Terminal Data

The terminal data elements listed in Table 11–2 are used for Card Risk Management. They are passed to the card in the first GENERATE AC command if they were included in the CDOL1 from the card. The CDOL1 requirements for the Card Risk Management checks are described in Table 11–1. The CDOL1 also includes tags for the data elements required for cryptogram generation.

For a detailed description of these elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables.

Table 11–2: Card Action Analysis—Terminal Data

Data Element	Description
Amount, Authorized	The amount of the transaction.
Transaction Currency Code	A code that indicates the currency of the transaction. This data element is requested by the card in the CDOL1.
Terminal Country Code	Terminal data indicating the country of the terminal. This data element is requested by the card in the CDOL1.
Terminal Verification Results (TVR)	A series of indicators used to record the results of offline processing from a terminal perspective including the results of all terminal risk management checks.

11.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command

The GENERATE APPLICATION CRYPTOGRAM (AC) command is used by the terminal to request that the card provide a cryptogram indicating the card's authorization response.

The P1 parameter of the GENERATE AC command indicates the type of cryptogram the terminal is requesting and whether the transaction is eligible for Combined DDA/AC Generation. The *EMV 4.0, Book 3*, Table I-12, shows the format of P1. The data portion of the command contains the data requested in the CDOL1.

When the card's CDOL1 data includes the tag for Terminal Capabilities, the transaction is eligible for Combined DDA/AC Generation if Terminal Capabilities in the GENERATE AC command data and the card's Application Interchange Profile (AIP) both indicate that Combined DDA/AC Generation is supported. Instead of using this method, VIS recommends explicitly requesting Combined DDA/AC Generation using the GENERATE AC command P1 parameter as described in the previous paragraph.

The command response includes the Application Cryptogram and the Cryptogram Information Data that shows the type of cryptogram being returned. If the transaction is eligible for Combined DDA/AC Generation and the cryptogram type is a TC or ARQC, the cryptogram returned is in an RSA public key envelope as described in the *EMV 4.0, Book 2*, Section 6.6.1.

11.4 Processing

11.4.1 Card Receives Cryptogram Request

The card receives the GENERATE AC command from the terminal. The data portion of the command contains the data elements which were requested in the CDOL1.

The data requirements for CDOL1 to support card risk management are described in Table 11–1 under the CDOL1 data description.

11.4.2 Card Risk Management

Table 11–3 summarizes the Card Risk Management checks provided, indicates whether they are mandatory, and describes the result if the condition being checked for occurs. The section of the chapter where the check is described is also provided.

If an issuer has elected to perform any of the optional Card Risk Management checks described below, the issuer needs to ensure that the data required to perform these checks is available to the card by personalizing the card with the appropriate data and ensuring that the appropriate tags and lengths for the terminal data are present in the CDOL1.

If a data object requested from the terminal is not available (in other words, the data object returned in the GENERATE AC command data field is zero filled), the card shall proceed to the next step in card risk management. If the Application Default Action (ADA) is not present in the card, the card shall use a default value of all zeros.

Table 11–3: Card Risk Management Checks (1 of 2)

Risk Management Check	Requirement	Result (If condition occurs)
Online Authorization Not Completed (on previous transaction) (Section 11.4.3.1)	Conditional—required if issuer script commands or Issuer Authentication are supported	Requests online processing and sets CVR indicator
Issuer Authentication Failure on Last Transaction (or Issuer Authentication Mandatory and not Performed on Last Transaction) (Section 11.4.3.2)	Conditional—required if Issuer Authentication supported	Sets Card Verification Results (CVR) indicator Checks Application Default Action (ADA) and requests online processing if indicated
Static Data Authentication (SDA) Failed on Last Transaction (Section 11.4.3.3)	Conditional—required if SDA supported	Sets CVR indicator
Dynamic Data Authentication (DDA) Failed on Last Transaction (Section 11.4.3.4)	Conditional—required if DDA supported	Sets CVR indicator

Table 11–3: Card Risk Management Checks (2 of 2)

Risk Management Check	Requirement	Result (If condition occurs)
Issuer Script Processed on Last Online Transaction (Section 11.4.3.5)	Conditional—required if Post-Issuance Updates supported	Provides number of script commands processed in CVR Sets CVR indicator if script processing failed (uses internal indicator Issuer Script Failure Indicator). ADA setting determines whether this failure results in online processing.
Velocity Checking for Total Consecutive Offline Transactions (Lower Limit) (Section 11.4.3.6)	Optional	Requests online processing if limit is exceeded and sets a CVR indicator.
Velocity Checking for Total Consecutive Offline International Transactions (Based on Currency) (Section 11.4.3.7)	Optional	Requests online processing if limit is exceeded and sets a CVR indicator.
Velocity Checking for Total Consecutive Offline International Transactions (Based on Country) (Section 11.4.3.8)	Optional	Requests online processing if limit is exceeded and sets a CVR indicator.
Velocity Checking for Transaction Amount in Designated Currency (Section 11.4.3.9)	Optional	Requests online processing if limit is exceeded and sets a CVR indicator.
Velocity Checking for Transaction Amount (Dual Currency) (Section 11.4.3.10)	Optional	Requests online processing if total cumulative amount of offline transactions in the designated or secondary currency since the last online transaction exceeded the limit. This check requires currency conversion if the transaction is in the secondary application currency. Also sets a CVR indicator.
New Card (Section 11.4.3.11)	Optional	May request online processing if no transactions have been processed online. Sets CVR indicator.
Offline PIN Verification not Performed (PIN Try Limit Exceeded) (Section 11.4.3.12)	Optional	Sets CVR indicator if Offline PIN Verification not Performed and the PIN Try Limit was previously exceeded. ADA setting determines whether this results in an offline decline or online processing.

11.4.3 Card Risk Management Processes

The card does each Card Risk Management check to see if the condition has occurred, then proceeds to the next check. If a check is not supported, the card proceeds to the next check.

11.4.3.1 Online Authorization Not Completed

This conditional check is required if Issuer Authentication or issuer script commands are supported. It determines whether during a previous transaction, the card was removed from the terminal after the card requested a online authorization and prior to receipt of an online response or terminal processing for unable to go online. This is shown by the Online Authorization Indicator that the card sets to "1" in a previous transaction when an online authorization is requested (see Chapter 13, Completion, for conditions under which this indicator is reset).

If the indicator is set, the card requests online processing until a transaction is sent online and one of the following is true:

- Issuer Authentication is successful
- Issuer Authentication is optional and not performed
- Issuer Authentication is not supported

NOTE: *This indicator is reset during Completion based on Issuer Authentication status and card parameters.*

If the Online Authorization Indicator is set to "1", the card:

- Sets the Online Requested by Card Indicator to "1".
- Sets the Last Online Transaction Not Completed bit to "1" in the CVR.

11.4.3.2 Issuer Authentication Failed (or Mandatory and Not Performed) on Last Transaction

This check is mandatory if Issuer Authentication is supported (as shown in the AIP). If Issuer Authentication (1) failed or (2) is mandatory (as shown in the Issuer Authentication Indicator) and was not performed on the last online transaction, online processing is requested by the card.

If the Issuer Authentication Failure Indicator is set to "1", the card:

- Sets the Issuer Authentication Failure on Last Online Transaction bit to "1" in the CVR.
- If the Application Default Action (ADA) bit for Issuer Authentication Failure, Transmit Next Transaction Online is "1", sets the internal Online Requested by Card Indicator to "1".

11.4.3.3 Static Data Authentication (SDA) Failed on Last Transaction

This check is mandatory if SDA is supported to check whether SDA failed on a previous offline declined transaction.

If the Static Data Authentication Failure Indicator is “1”, the card sets the Offline Static Data Authentication Failed on Last Transaction and Transaction Declined Offline bit to “1” in the CVR.

11.4.3.4 Dynamic Data Authentication (DDA) Failed on Last Transaction

This check is mandatory if DDA is supported to check whether DDA failed on a previous offline declined transaction.

If the Dynamic Data Authentication Failure Indicator is “1”, the card sets the Offline Dynamic Data Authentication Failed on Last Transaction and the Transaction Declined Offline bit to “1” in the CVR.

11.4.3.5 Issuer Script Processed on Last Online Transaction

This check is mandatory if Issuer Script processing is supported. It provides the issuer with a count of the number of issuer script commands processed on the last online transaction and indicates whether script processing failed.

The card shall set bits 8–5 in the fourth byte of the CVR to the value of the Issuer Script Command Counter using identical bit settings.

If the Issuer Script Failure Indicator is set to “1”, the card sets the Issuer Script Processing Failed on Last Transaction bit to “1” in the CVR.

If the Issuer Script Failure Indicator is set to “1” and the ADA bit for If Issuer Script Failed on Previous Transaction, Transmit Transaction Online is set to “1”, set the Online Requested by Card Indicator to “1”.

11.4.3.6 Velocity Checking for Total Consecutive Offline Transactions (Lower Limit)

This optional card check generates a request for an online authorization if the limit for the number of total consecutive offline transactions has been exceeded.

The card shall perform this check if the Last Online ATC Register is present in the card and the Visa proprietary Lower Consecutive Offline Limit (tag “9F58”) is present in a proprietary internal card file.

If the difference between the ATC and the Last Online ATC Register is greater than the Lower Consecutive Offline Limit, the card:

- Sets the Exceeded Velocity Checking Counters bit to "1" in the CVR.
- Sets the Online Requested by Card Indicator to "1" to request that an ARQC should be returned after completion of Card Risk Management.

11.4.3.7 Velocity Checking for Total Consecutive Offline International Transactions (Based on Currency)

This optional card check generates a request for an online authorization if the limit on the number of consecutive international offline transactions has been exceeded. This check defines an international transaction as a transaction where the Transaction Currency Code from the terminal does not match the Application Currency Code on the card.

The card shall perform this check if the Application Currency Code, Consecutive Transaction Counter (International), and Consecutive Transaction Limit (International) are present.

The card compares the Transaction Currency Code to the Application Currency Code. If they are not equal and the Consecutive Transaction Counter (International) plus 1 is greater than the Consecutive Transaction Limit (International), the card:

- Sets the Exceeded Velocity Checking Counters bit to "1" in the CVR.
- Sets the Online Requested by Card Indicator to "1".

11.4.3.8 Velocity Checking for Total Consecutive International Transactions (Based on Country)

This optional card check generates a request for an online authorization if the limit on the number of international offline transactions since the last online approval has been exceeded. This check defines an international transaction as one where the Terminal Country Code does not match the card's Issuer Country Code.

The card shall perform this check if the Issuer Country Code, Consecutive Transaction Counter (International—Country), and Consecutive Transaction Limit (International—Country) are present.

If *both* of the following conditions are true:

- The Terminal Country Code does not match the Issuer Country Code:
- One plus the Consecutive Transaction Counter (International—Country) is greater than the Consecutive Transaction Limit (International—Country)

the card:

- Sets the Exceeded Velocity Checking Counters bit to “1” in the CVR.
- Sets the Online Requested by Card Indicator to “1”.

11.4.3.9 Velocity Checking for Transaction Amount in Designated Currency

This optional card check generates a request for an online authorization if the limit on the amount accumulated for consecutive offline approved transactions performed in the application's designated currency has been exceeded.

The card shall perform this check if the Application Currency Code, Cumulative Total Transaction Amount and Cumulative Total Transaction Amount Limit are present.

If *both* of the following conditions are true:

- The Transaction Currency Code is the same as the Application Currency Code:
- The sum of the Cumulative Total Transaction Amount and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Limit

the card:

- Sets the Exceeded Velocity Checking Counters bit to “1” in the CVR.
- Sets the Online Requested by Card Indicator to “1”.

11.4.3.10 Velocity Checking for Transaction Amount (Dual Currency)

This optional card check generates a request for an online authorization if the limit on the amount accumulated for consecutive offline approved transactions performed in the application's designated application currency or a second designated currency has been exceeded.

The card shall perform this check if the Application Currency Code, Secondary Application Currency Code, Currency Conversion Factor, Cumulative Total Transaction Amount (Dual Currency), and Cumulative Total Transaction Amount Limit (Dual Currency) are present.

- If the Transaction Currency Code equals the Application Currency Code, the sum of the Cumulative Total Transaction Amount (Dual Currency) and the Amount, Authorized is compared to the Cumulative Total Transaction Amount Limit (Dual Currency)
- If the Transaction Currency Code equals the Secondary Application Currency Code, the Amount, Authorized and the Currency Conversion Factor are used to determine the approximate value of the transaction in the application currency. The sum of this approximate value and the Cumulative Total Transaction Amount (Dual Currency) is compared to the Cumulative Total Transaction Amount Limit (Dual Currency)
- If the comparison shows the Cumulative Total Transaction Amount Limit (Dual Currency) to be exceeded, the card shall:
  - Set the Exceeded Velocity Checking Counters bit to “1” in CVR.
  - Set the Online Requested by Card Indicator to “1”.

EXAMPLE

Converting Euros to French Francs:

- The French Franc is the designated Application Currency.
- The Euro is the Secondary Application Currency.
- Conversion rate is 6.56 French Francs to a Euro.
- Currency Conversion Factor is 10000066

  (first nibble indicates decimal is 1 digit from right;

  last 7 nibbles of 0000066 represent 6.56 reduced to two significant digits).
- Amount Authorized is 50.00 Euros (5000 with an implied 2 decimal places).
- Cumulative Total Transaction Amount prior to transaction is 80000 (800.00 French Francs)
- Cumulative Total Transaction Amount Limit is 100000 (1000.00 French Francs).

Step 1. Multiply 5000 (Amount Authorized in Euros) by 66 (Currency Conversion Factor without first nibble) to get 330000.

Step 2. Adjust by 1 (the first nibble of Currency Conversion Factor) to get 33000 (330.00 Francs).

Step 3. Compare 33000 plus 80000 (Cumulative Total Transaction Amount (Dual Currency)) to 100000 (Cumulative Total Transaction Amount Limit (Dual Currency)). The limit is exceeded.

11.4.3.11 New Card

This optional card check generates a request for an online authorization if the card is a new card. A new card is a card that has never been approved online.

The card shall perform this check if the Last Online ATC Register and Application Default Action are present in the card.

If the Last Online ATC Register is zero, the card:

- Sets the New Card bit to "1" in the CVR.
- If the Application Default Action (ADA) bit for If New Card, Transmit Transaction Online bit is set to "1", set the Online Requested by Card Indicator to "1".

NOTE: *If Issuer Authentication is mandatory on the card, the Last Online ATC Register remains zero until Issuer Authentication is successful.*

11.4.3.12 Offline PIN Verification Not Performed (PIN Try Limit Exceeded)

This optional check for cards supporting Offline PIN verification generates a request for an online authorization if the PIN Try Limit has been exceeded on a previous transaction.

If this check is to be performed, the Application Default Action shall be present in the card.

If *all* of the following are true:

- The card supports Offline PIN verification
- A VERIFY command was not received from the terminal
- The PIN Try Counter equals zero

the card shall perform the following actions:

- Set PIN Try Limit Exceeded in the CVR.
- If Application Default Action (ADA) bit for If PIN Try Limit Exceeded on Previous Transaction, Decline Transaction equals "1", set Offline Decline Requested by Card Indicator to "1"
- If ADA bit for If PIN Try Limit Exceeded on Previous Transaction, Go Online equals "1", set Online Requested by Card Indicator to "1"
- If ADA bit for If PIN Try Limit Exceeded on Previous Transaction, Decline and Block Application equals "1", decline the transaction and block the application

11.5 Card Provides Response Cryptogram

Based on the results of this Card Risk Management, the card responds to the GENERATE AC command issued by the terminal. The card's response may override the cryptogram type designated by the terminal in the P1 parameter of the first GENERATE AC command according to the following rules:

- The card may override the terminal's decision to approve offline by deciding to either send online or decline offline.
- The card may override the terminal's decision to go online by deciding to decline offline.

These decision rules are shown in Table 11–4.

Table 11–4: Card's Response to First GENERATE AC Command

		Card Responds		
		AAC	**ARQC**	**TC**
Terminal Requests	**AAC**	Decline	—	—
	ARQC	Decline	Go Online	—
	TC	Decline	Go Online	Approve

The card's decision to decline offline is indicated by the Offline Decline Requested by Card Indicator equal to "1". The card's decision to go online is indicated by the Online Requested by Card Indicator equal to "1".

NOTE: *In this version of the Visa Integrated Circuit Card Specification, the card shall never respond with an AAR (referral).*

The card sets the CVR to indicate that a TC (offline approval), AAC (offline decline), or ARQC (go online for authorization) is to be returned in response to the first GENERATE AC and that a second GENERATE AC has not been requested.

The card generates a DES-based cryptogram utilizing the data provided by the terminal and data from the card. Data requirements are detailed in Appendix E, Cryptogram Versions Supported. The key requirements and the algorithms used in the cryptogram generation process are detailed in Appendix D, Authentication Keys and Algorithms.

Additional card processing for each response decision is outlined in the following sections.

11.5.1 Card Declined Transaction Offline

When the transaction is to be declined offline, the card shall respond to the GENERATE AC command with an AAC. Prior to responding, the card:

1. Checks the Application Default Action (ADA):
   - If the ADA bit for If Transaction Declined Offline, Create Advice = "1", set Advice Required to "1" in the Cryptogram Information Data (CID)
   - If PIN Try Limit has been exceeded on this transaction and the ADA indicates that an advice is required when this occurs:
     - Set Advice Required = "1" in the CID
     - If the CID reason code is not set to "Service not allowed", set the CID reason code to "PIN Tries Exceeded"

     NOTE: *The service not allowed code in the CID takes precedence over all other reason codes.*
2. Checks the TVR provided by the terminal in the GENERATE AC command:
   - If Static Data Authentication Failed bit = "1", set the Static Data Authentication Failure Indicator to "1"
   - If Dynamic Data Authentication Failed bit = "1" or Combined DDA/AC Generation Failed bit = "1", set the Dynamic Data Authentication Failure Indicator to "1"
3. Increments counters, if present, as follows:
   - If the Terminal Country Code is not equal to the Issuer Country Code, increment the Consecutive Transaction Counter (International—Country) by 1
   - If the Transaction Currency Code is not equal to the Application Currency Code, increment the Consecutive Transaction Counter (International) by 1

11.5.2 Card Requested Online Processing

When the transaction is to go online for an authorization, the card shall respond to the GENERATE AC command with an ARQC. Prior to responding, the card sets the Online Authorization Indicator to "1".

NOTE: *The following counters are **not** incremented at this time: Consecutive Transaction Counter (International—Currency), Consecutive Transaction Counter (International—Country), Cumulative Total Transaction Amount, or Cumulative Total Transaction Amount (Dual Currency).*

11.5.3 Card Approved Transaction Offline

When the transaction is to be approved offline, the card shall respond to the GENERATE AC command with a Transaction Certificate (TC). Prior to responding, the card increments counters, if present, as follows:

- If the Terminal Country Code is not equal to the Issuer Country Code, increment the Consecutive Transaction Counter (International—Country) by 1
- If the Transaction Currency Code is equal to the Application Currency Code:
  - Increment the Cumulative Total Transaction Amount by the Amount, Authorized
  - Increment the Cumulative Total Transaction Amount (Dual Currency) by the Amount, Authorized
- If the Transaction Currency Code is not equal to the Application Currency Code, increment the Consecutive Transaction Counter (International) by 1
- If the Transaction Currency Code is equal to the Secondary Application Currency Code, increment the Cumulative Total Transaction Amount (Dual Currency) by the amount converted to the Application Currency using the Amount, Authorized and the Currency Conversion Factor

11.5.4 Combined DDA/AC Generation Requested

The terminal requests Combined DDA/AC Generation when one of the following occurs:

- The card's CDOL1 contains the tag for Terminal Capabilities and the Terminal Capabilities returned in the GENERATE AC command and the card's Application Interchange Profile both indicate support for Combined DDA/AC Generation.
- The card's CDOL1 does not contain the tag for Terminal Capabilities and the Combined DDA/AC Generation bit of the GENERATE AC command's P1 parameter is set to "1".

Upon determining that the terminal is requesting Combined DDA/AC Generation, the card shall:

1. Perform standard Card Risk Management and generate the Application Cryptogram as described above.
2. If the card's response is an AAC, return the AAC in the GENERATE AC response as shown in the *EMV 4.0, Book 3*, Table I-13.
3. If the card's response is an ARQC or TC, the card returns the Application Cryptogram in an RSA envelope as follows:
   a. Set the Offline Dynamic Data Authentication Performed bit to "1" in the Card Verification Results (CVR). This bit shall be set prior to the generation of the Application Cryptogram in Step 1.
   b. Generate a dynamic signature from the Application Cryptogram as described in the *EMV 4.0, Book 2*, Section 6.6.1, and summarized in the next four steps:
      - Concatenate the data indicated in Table 14 of the *EMV 4.0, Book 2*. This data includes the ICC Dynamic Data containing the ICC Dynamic Number Length, ICC Dynamic Number, Cryptogram Information Data, and the Application Cryptogram.
      - Generate a hash value from the data concatenated above.
      - Include the hash in the Signed Dynamic Application Data.
      - Sign the Signed Dynamic Application Data with the ICC Private Key.
   c. Include the Signed Dynamic Application Data in the GENERATE AC response.

11.6 Processing Flow

Figure 11–1: Card Action Analysis Processing Flow (1 of 6)

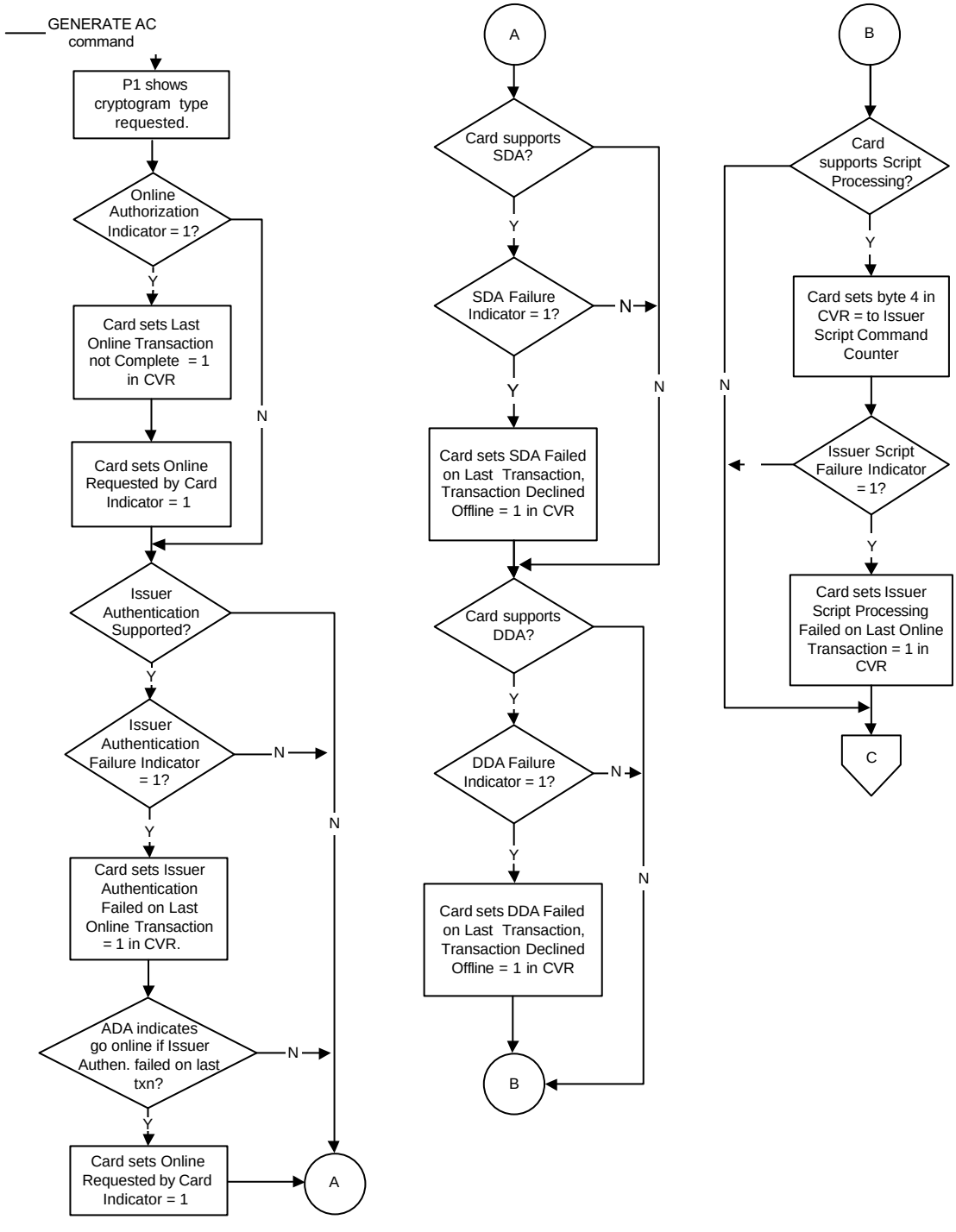


Figure 11–2: Card Action Analysis Processing Flow (2 of 6)

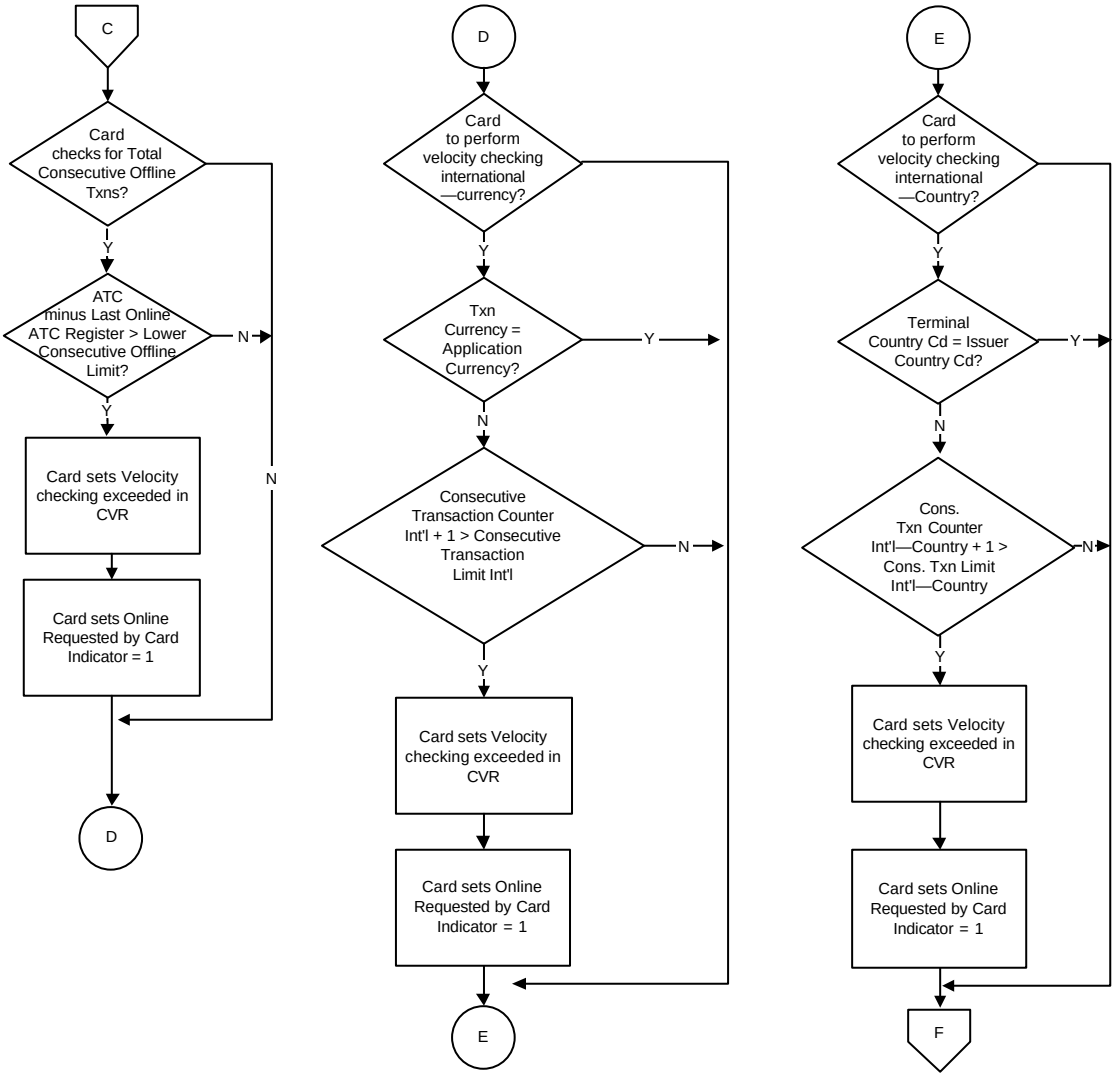


Figure 11–3: Card Action Analysis Processing Flow (3 of 6)

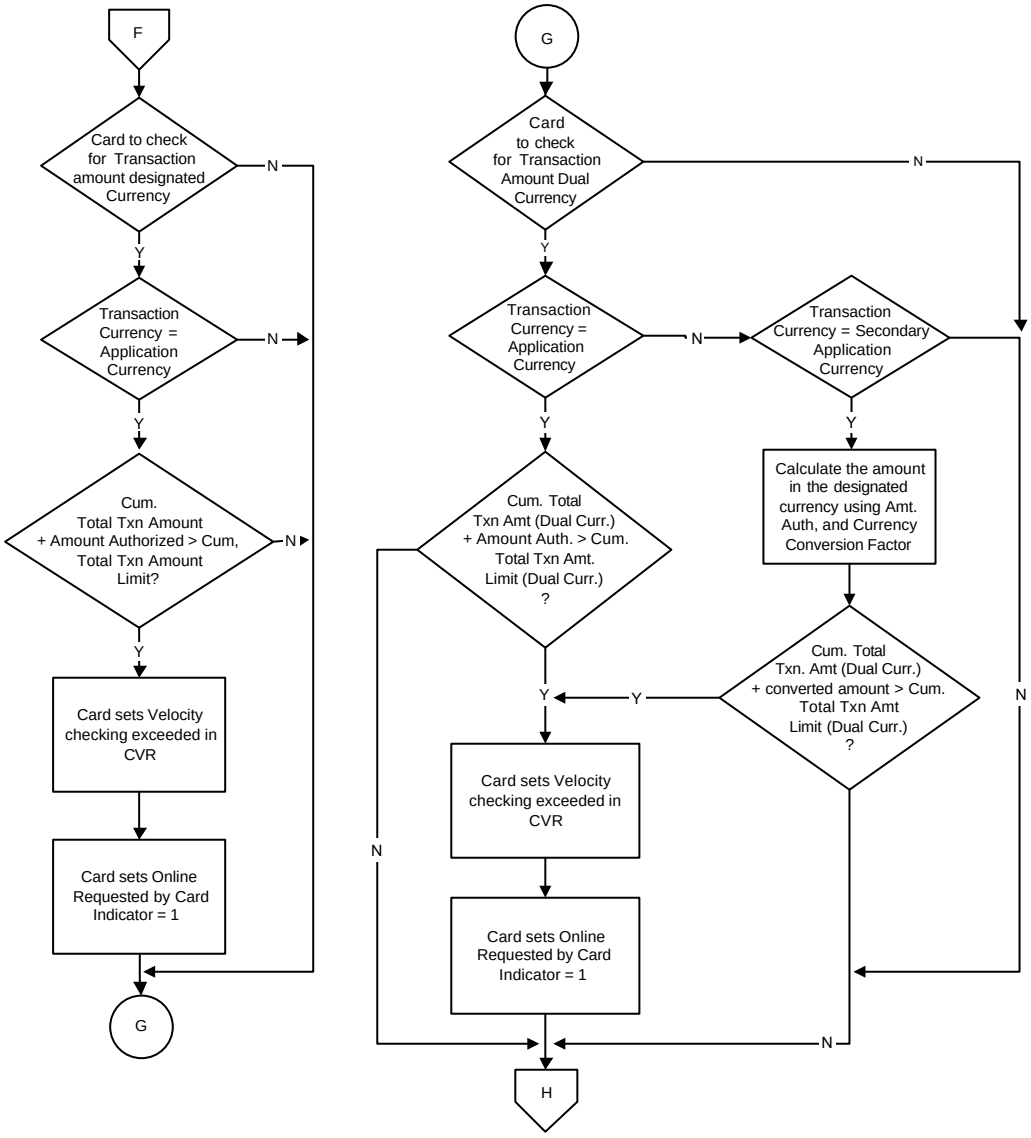


Figure 11–4: Card Action Analysis Processing Flow (4 of 6)

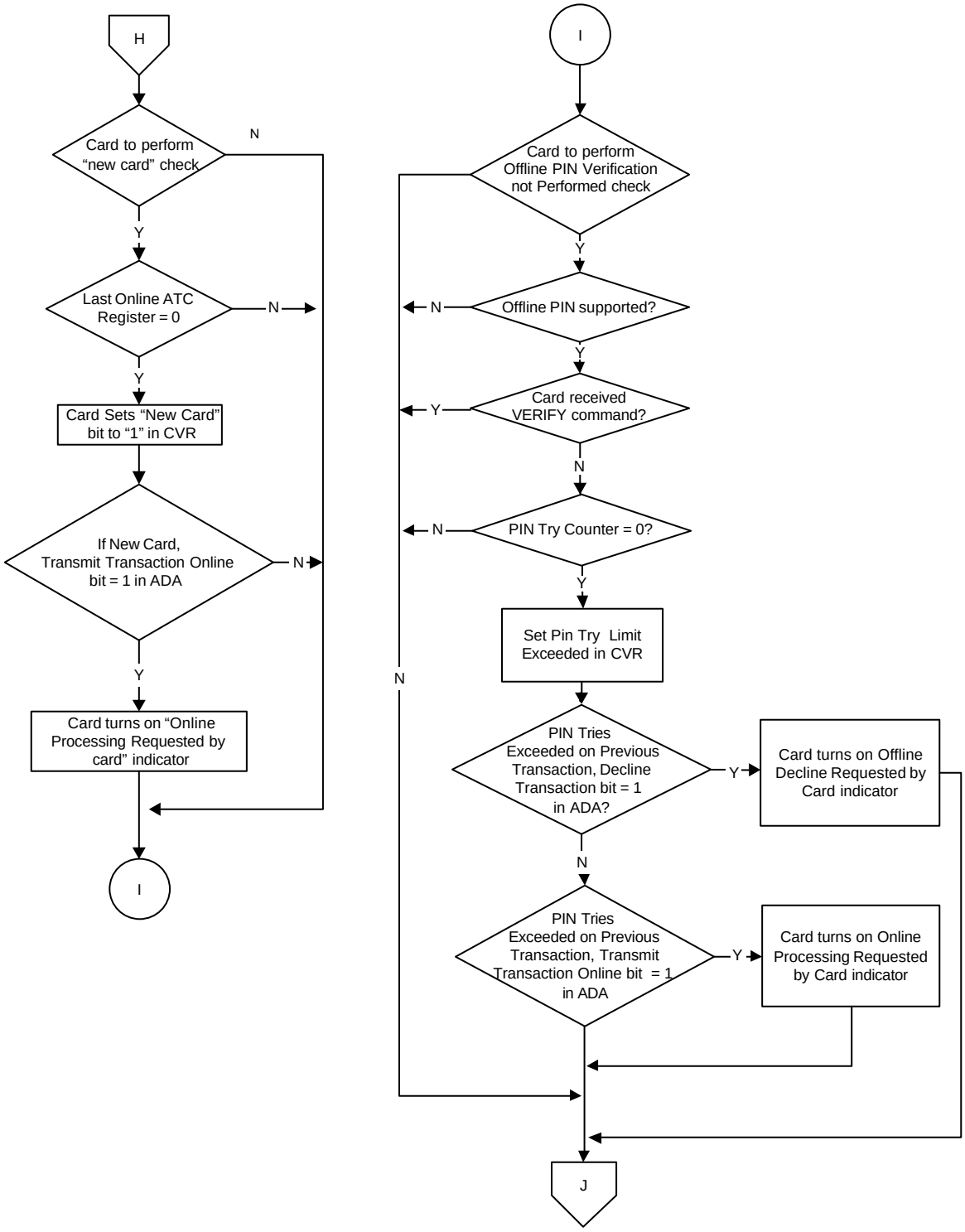


Figure 11–5: Card Action Analysis Processing Flow (5 of 6)

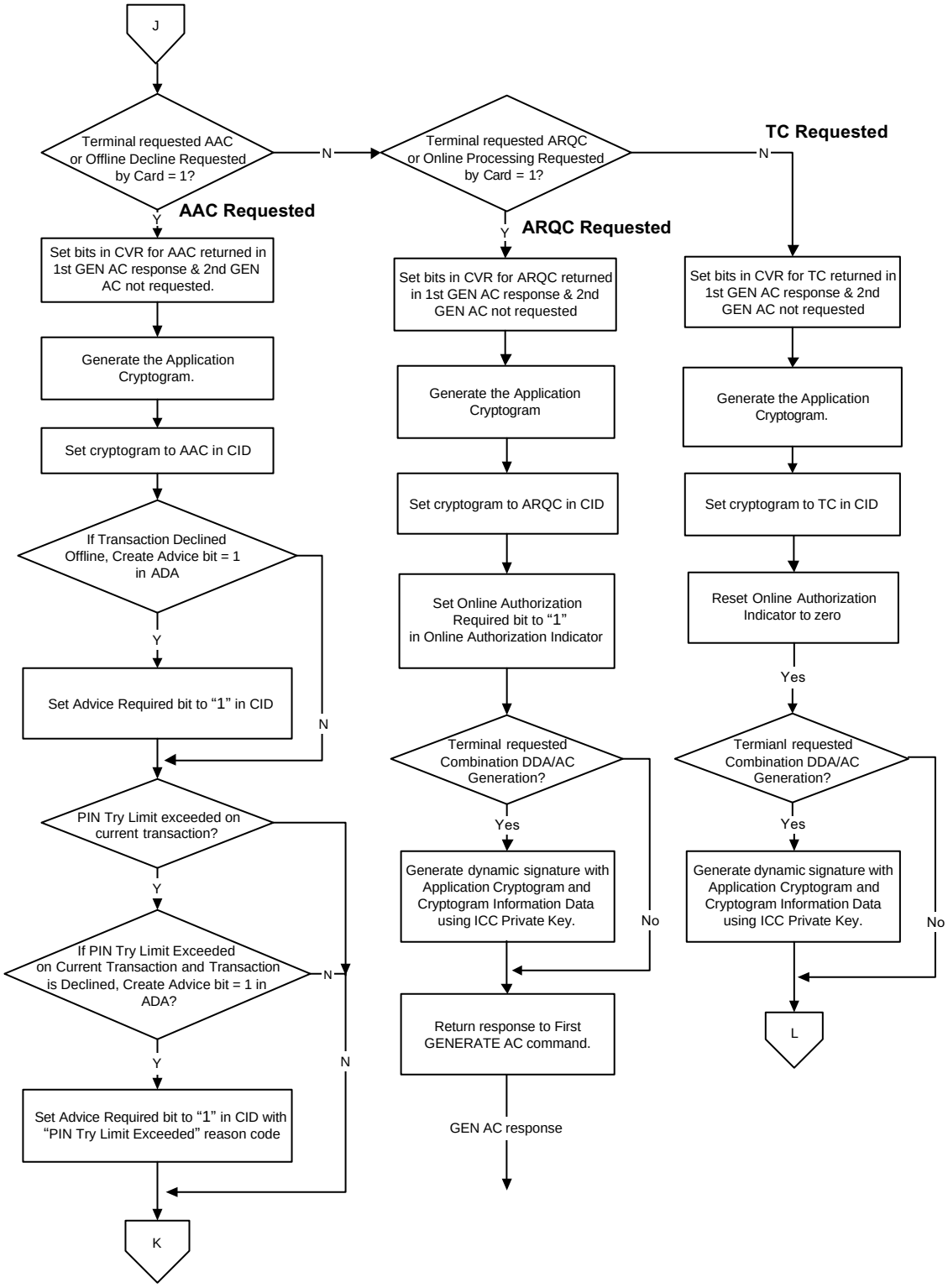
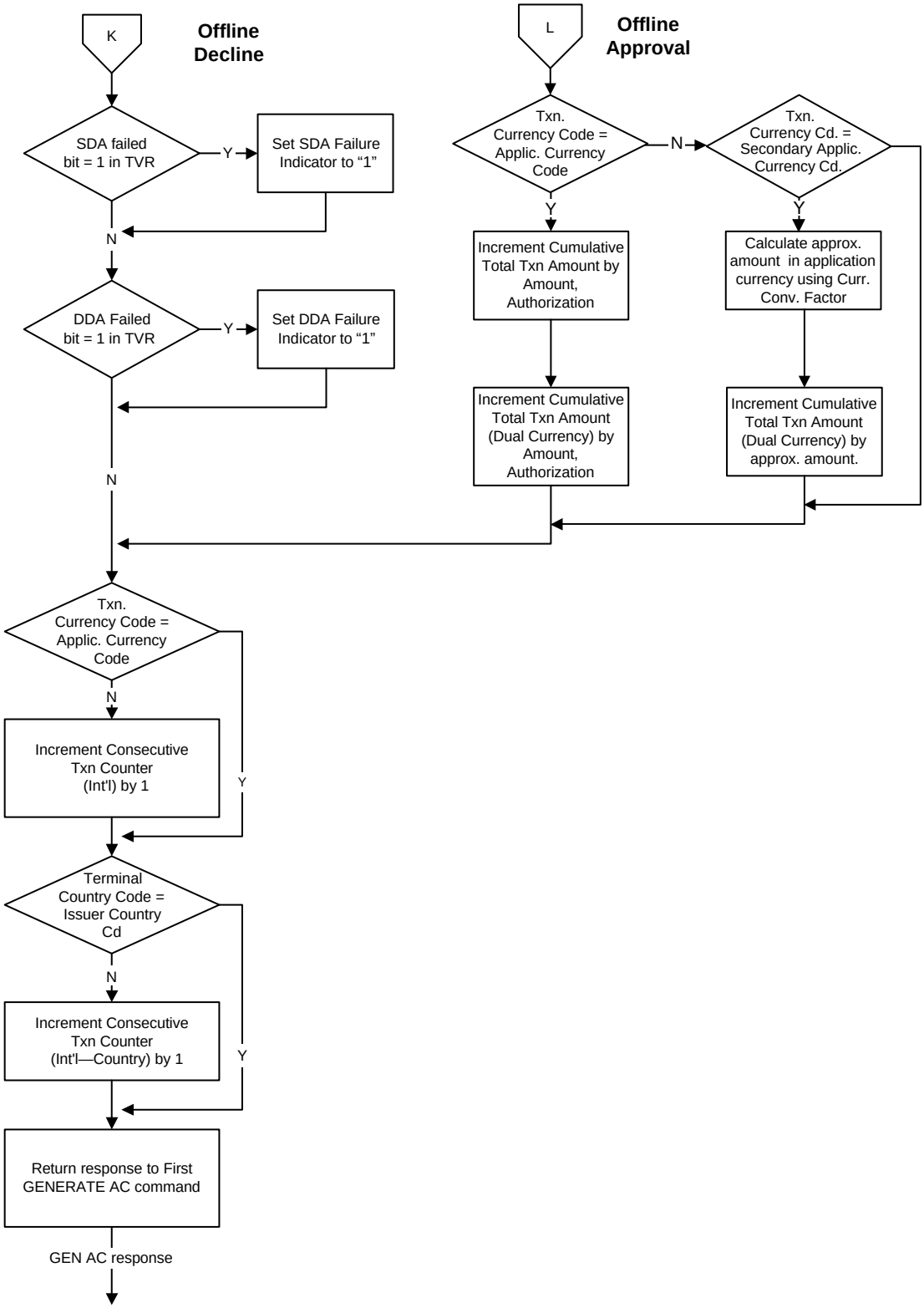


Figure 11–6: Card Action Analysis Processing Flow (6 of 6)



11.7 Prior Related Processing

Read Application Data

The terminal reads the CDOL1 from the card.

Terminal Action Analysis

The terminal issues the First GENERATE AC command to the card to request a cryptogram. The command includes the data requested in the CDOL1 including the data required for the cryptogram generation and Card Risk Management.

11.8 Subsequent Related Processing

Online Processing

The terminal uses the cryptogram type specified in the Cryptogram Information Data (CID) of the first GENERATE AC response to determine whether to perform an online authorization.

Completion

If online processing was requested but the terminal was unable to send the transaction online, additional card risk management checks are performed.

Indicators and counters used in Card Action Analysis are reset based upon Issuer Authentication status and card options regarding Issuer Authentication.

Online Processing 12

Online Processing allows the issuer's host computer to review and authorize or decline transactions using the issuer's host-based risk management parameters. In addition to performing traditional online fraud and credit checks, host authorization systems may perform Online Card Authentication using a card-generated dynamic cryptogram and may consider offline processing results in the authorization decision.

The response from the issuer may include post-issuance updates to the card and an issuer-generated cryptogram that the card can validate to assure that the response came from the valid issuer. This validation is called Issuer Authentication.

This chapter describes the card online processing functions that are new with Visa Smart Debit and Visa Smart Credit (VSDC). Online processing functions that are also performed with magnetic stripe-read and key-entered transactions are not described.

Online processing shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 6.9, and *Book 4*, Section 2.3.8.

This chapter is organized into these sections:

12.1 Card Data

12.2 Online Response Data

12.3 EXTERNAL AUTHENTICATE Command

12.4 Processing

12.5 Processing Flow

12.6 Prior Related Processing

12.7 Subsequent Related Processing

12.1 Card Data

The terminal uses the data from the card, described in Table 12–1, during processing of the online request. For a detailed description of these card data elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 12–1: GENERATE AC Response—Card Data

Data Element	Description
Cryptogram Information Data (CID)	Contains an indicator of the type of cryptogram. For transactions to be authorized online, the cryptogram type is an ARQC (Authorization Request Cryptogram). An ARQC is designated by “10” in the first two bits (bits 8–7) of this field.
Application Transaction Counter	Counter of transactions initiated with the card application since the application was put on the card.
Application Cryptogram	The online cryptogram (ARQC) value from the card.
Issuer Application Data	Issuer Application Data is a Visa-mandatory field used to transmit Visa discretionary data to the terminal for input to the online request message or clearing record. The coding of Issuer Application Data is described in Appendix A, Card and Issuer Data Element Tables. It contains the following data concatenated in the order specified: • Length Indicator • Derivation Key Index (DKI) • Cryptogram Version Number • Card Verification Results (CVR) • Issuer Discretionary Data (optional) The length indicator, DKI, Cryptogram Version Number, and CVR are mandatory, while the Issuer Discretionary Data is optional when the card returns an ARQC. Although national markets may support the Issuer Discretionary Data in the online request, the Issuer Discretionary Data may not be available in international interchange. The amount of discretionary data that may be included in an online request will be determined by national markets and is outside the scope of the *Visa Integrated Circuit Card Specification*.

After receipt of the online response, the terminal uses the data described in Table 12–2 from the card.

Table 12–2: Issuer Authentication Decision—Card Data

Data Element	Description
Application Interchange Profile (AIP)	The AIP was sent to the terminal by the card during Initiate Application Processing. The AIP bit for Issuer Authentication shall be set to “1” if the card supports Issuer Authentication.

The card uses the data described in Table 12–3 during the Issuer Authentication portion of Online Processing.

Table 12–3: Online Processing, Issuer Authentication—Card Data

Data Element	Description
Authorization Request Cryptogram (ARQC)	The cryptogram calculated by the card during Card Action Analysis that is input to the Authorization Response Cryptogram (ARPC) validation.
Card Verification Results (CVR)	The CVR contains the following flags related to Issuer Authentication: • Issuer Authentication Performed and Failed • Issuer Authentication Failure on Last Online Transaction • Issuer Authentication Not Performed after Online Authorization.
Issuer Authentication Failure Indicator	The card sets the Issuer Authentication Failure Indicator to “1” if Issuer Authentication fails.
Unique DEA Key A and B (UDKs)	The card’s secret DES keys which the card uses to validate the ARPC.

12.2 Online Response Data

The online response from the issuer to the terminal contains the data described in Table 12–4. The terminal passes this data to the card in the EXTERNAL AUTHENTICATE command for use during Issuer Authentication. In addition to the data shown, the online response may contain Issuer Script data as described in Chapter 14, Issuer-to-Card Script Processing.

Table 12–4: Online Processing—Terminal Data

Data Element	Description
Issuer Authentication Data	Data that the terminal includes in the EXTERNAL AUTHENTICATE command sent to the card. As described in the *EMV 4.0, Book 3*, Section 2.5.4.3, the first eight bytes contain the mandatory Authorization Response Cryptogram (ARPC) followed by an optional 1–8 bytes of which this version of the *Visa Integrated Circuit Card Specification* uses 2. In this version, the Issuer Authentication Data consists of the following data: • Authorization Response Cryptogram (ARPC)—The cryptogram generated by the issuer host (or its agent) and passed to the terminal in the online response. • Authorization Response Code—The response code used in the calculation of the ARPC and passed to the terminal in the online response from the issuer. ***Note:*** *Optional Issuer data is not supported in this version of the* Visa Integrated Circuit Card Specification.

12.3 EXTERNAL AUTHENTICATE Command

EXTERNAL AUTHENTICATE Command

The EXTERNAL AUTHENTICATE command is sent to the card by the terminal when Issuer Authentication should be performed. This command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.4 and Appendix B, Secure Messaging, in this document.

The EXTERNAL AUTHENTICATE command contains the Issuer Authentication Data from the online response.

The EXTERNAL AUTHENTICATE response from the card contains the pass/fail results of the validation of the Issuer Authentication Data. SW1 SW2 equals “9000” when Issuer Authentication passes and equals “6300” when Issuer Authentication fails.

The card shall permit at most one EXTERNAL AUTHENTICATE command in a transaction. All succeeding EXTERNAL AUTHENTICATE commands shall return SW1 SW2 = “6985”.

12.4 Processing

Online Processing has up to three components: online request processing, online response processing, and Issuer Authentication. The card only performs processing during the Issuer Authentication step.

12.4.1 Online Request

The terminal initiates an online request if it receives an Authorization Request Cryptogram (ARQC) from the card after Card Action Analysis in the GENERATE APPLICATION CRYPTOGRAM (AC) response and the terminal supports online authorizations. The online request contains data previously received from the card, but the card plays no role in the transmission of the online request to the issuer.

12.4.2 Online Response

The card plays no role in the receipt of the online response from the issuer.

12.4.3 Issuer Authentication

The terminal sends an EXTERNAL AUTHENTICATE command to the card if the Application Interchange Profile (AIP) from the card indicates Issuer Authentication is supported and the online response contains Issuer Authentication Data.

When the card receives an EXTERNAL AUTHENTICATE command from the terminal, the card shall perform Issuer Authentication using the following steps:

1. If an EXTERNAL AUTHENTICATE command was previously received during the current transaction:
   - Set Issuer Authentication Failure Indicator to “1”.
   - Respond to terminal with SW1 SW2 = “6985”.
2. Parse out the Authorization Response Code included in the Issuer Authentication Data and store it for later use during the Completion processing function.
3. Generate an Authorization Response Cryptogram (ARPC) from the Authorization Response Code and the ARQC returned with the first GENERATE AC response using the algorithm described in Appendix D, Authentication Keys and Algorithms, and the Unique DEA Keys (UDKs) stored in the card for the application.
4. Compare the generated ARPC to the ARPC received in the EXTERNAL AUTHENTICATE command. If they are the same, Issuer Authentication is considered successful.

If Issuer Authentication is successful, the card shall:

1. Set the Issuer Authentication Failure Indicator to “0”.
2. Indicate that Issuer Authentication was successful in the EXTERNAL AUTHENTICATE command response sent to the terminal (SW1 SW2 = “9000”).

If Issuer Authentication fails, the card shall:

1. Set the Issuer Authentication Failure Indicator to “1”.
2. Set the Issuer Authentication Performed and Failed bit to “1” in the CVR.
3. Indicate that Issuer Authentication failed in the EXTERNAL AUTHENTICATE command response sent to the terminal (SW1 SW2 = “6300”).

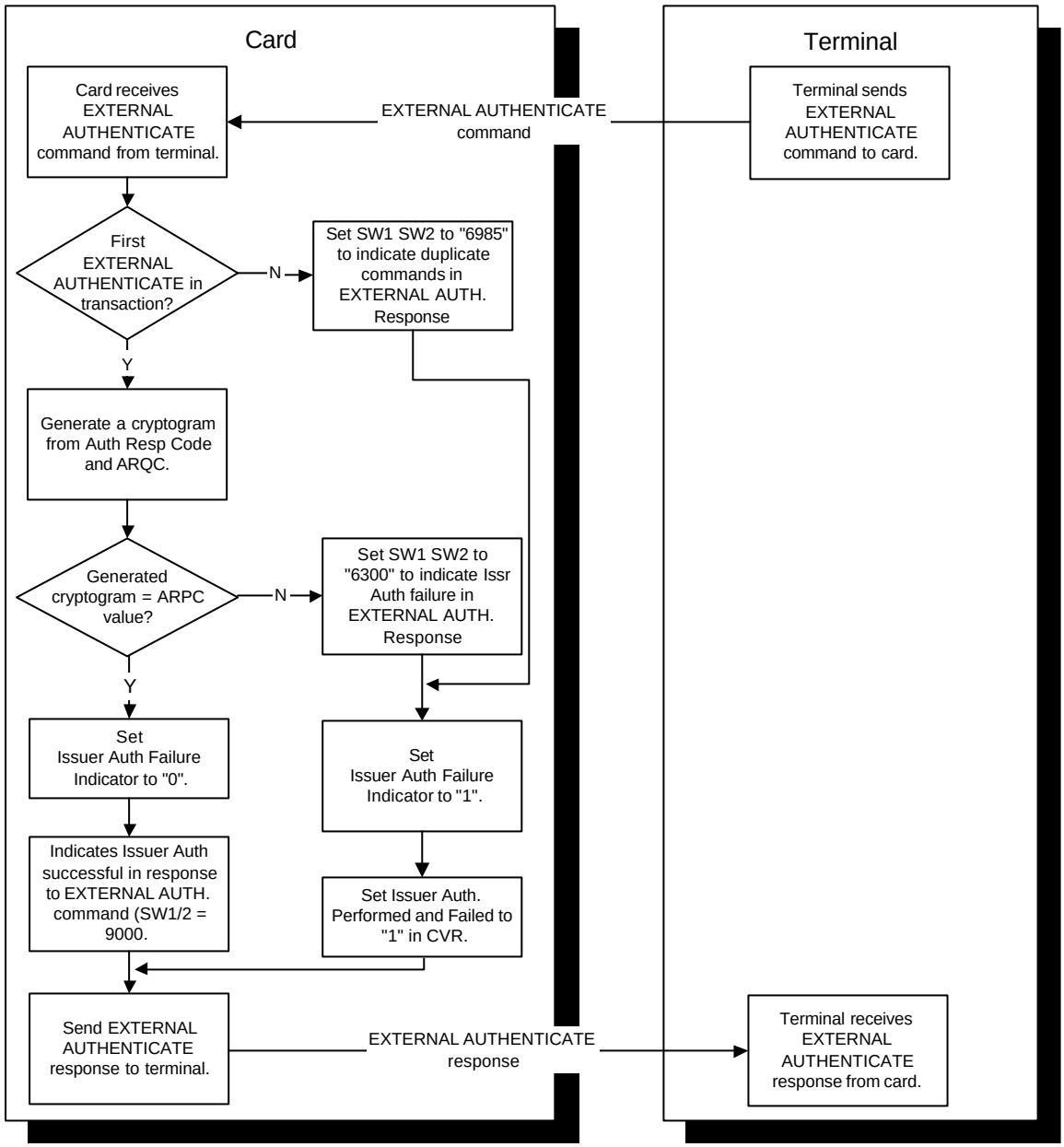
The card shall ensure that the Issuer Authentication Failure Indicator remains set to "1" when it is removed from the terminal after the completion of the transaction. During the next transaction, the card shall check this indicator during Card Action Analysis to determine if that transaction should be transmitted online.

During Completion processing, the card shall be able to determine if Issuer Authentication was performed and successful for the transaction since the response to the final GENERATE APPLICATION CRYPTOGRAM may be dependent upon these results.

12.5 Processing Flow

Figure 12–1 shows how the card could perform Issuer Authentication during Online Processing.

Figure 12–1: Online Processing Flow



12.6 Prior Related Processing

Initiate Application Processing

The card sends the AIP to the terminal in response to the GET PROCESSING OPTIONS command. The AIP indicates whether the card supports Issuer Authentication.

Card Action Analysis

The card returns the Application Cryptogram in response to the first GENERATE AC command.

12.7 Subsequent Related Processing

Completion

During Completion, the card uses the results of Issuer Authentication to determine the transaction disposition and whether to reset certain counters and indicators.

Issuer-to-Card Script Processing

The terminal sends any issuer script commands received in the online response to the card. The card may consider Issuer Authentication results in deciding whether to apply issuer scripts.

Card Action Analysis (Subsequent Transactions)

If the Online Authorization Indicator is set indicating that online processing did not complete on a previous transaction, the card will send the transaction online for an authorization.

Completion 13

Completion is performed by the terminal and the card to conclude transaction processing. Completion includes the following:

- If online processing was requested and the terminal did not support online processing or the online authorization was unable to complete, the terminal and card perform additional analysis to determine whether the transaction should be approved or declined offline.
- An issuer's online approval may be changed to a decline based upon Issuer Authentication results and card options.
- Indicators and counters are set to reflect what has occurred during transaction processing.
- After an online authorization, indicators and counters may be reset based upon Issuer Authentication status and card options.

Completion shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3,* Section 6.11, and *Book 4,* Section 8.2.1.

This chapter is organized as follows:

13.1 Card Data

13.2 Terminal Data

13.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command

13.4 Completion Processing Overview

13.5 Receive GENERATE AC Command

13.6 Transaction Authorized Online

13.7 Online Processing Requested, Online Authorization Not Completed

13.8 Completion Processing Transaction Flow

13.9 Prior Related Processing

13.10 Subsequent Related Processing

13.1 Card Data

The card uses the card data described in Table 13–1 internally during Completion. For a detailed description of these data elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 13–1: Completion—Card Data (1 of 2)

Data Element	Description
Application Currency Code (“9F51”)	Indicates the currency in which the account is managed.
Application Default Action (ADA)	A Visa proprietary data element indicating the issuer-specified action a card should take when exception conditions occur.
Application Interchange Profile (AIP)	Indicates ability of the card to support specific functions including Issuer Authentication.
Consecutive Transaction Counter (International)	A Visa proprietary data element specifying the number of transactions that have occurred offline for the card application in a currency other than the application currency since the last online authorization.
Consecutive Transaction Counter (International—Country)	A Visa proprietary data element specifying the number of international transactions that have occurred offline for the card application since the last online authorization. This check uses the Issuer Country Code to determine domestic versus international transactions.
Cumulative Total Transaction Amount	A Visa proprietary data element specifying the total accumulated amount for offline approved transactions in the designated currency (Application Currency Code) since the last online approved transaction.
Cumulative Total Transaction Amount (Dual Currency)	A Visa proprietary data element specifying the total accumulated amount for offline approved transactions in the designated currency (Application Currency Code) or a secondary currency (Secondary Application Currency Code) since the last online approved transaction. Amounts in the secondary currency are converted to the designated currency using the Currency Conversion Factor prior to being accumulated.
Cumulative Total Transaction Amount Upper Limit	A Visa proprietary data element specifying the limit on the total accumulated amount in either the designated currency (Application Currency Code) or in the designated and secondary currency (Secondary Application Currency Code) since the last online approved transaction.

Table 13–1: Completion—Card Data (2 of 2)

Data Element	Description
Currency Conversion Factor	The relationship between the application (designated) currency (Application Currency Code) and the secondary currency (Secondary Application Currency Code). Amounts in the secondary currency are multiplied by the Currency Conversion Factor to determine their approximate value in the application currency.
Dynamic Data Authentication Failure Indicator	Indicates that DDA failed during the current or a previous transaction.
Issuer Authentication Failure Indicator	Indicates that Issuer Authentication failed during the current or a previous transaction. This indicator is used in Card Action Analysis on following transactions.
Issuer Authentication Indicator	Indicates whether Issuer Authentication is mandatory or optional for this card. When Issuer Authentication is set as mandatory, the card must receive and successfully process an ARPC (that is, pass Issuer Authentication) in order for the Last Online ATC Register and the offline counters to be reset.
Issuer Country Code (“9F57”)	Indicates the country of the issuer.
Issuer Script Command Counter	Indicates the number of issuer script commands requiring secure messaging received by the card after the second GENERATE AC command of a previous transaction.
Issuer Script Failure Indicator	Indicates that Issuer Script has failed during a previous transaction and results have not yet been sent to the Issuer.
Last Online ATC Register	ATC value of the last transaction that was authorized online and satisfied Issuer Authentication requirements.
Online Authorization Indicator	Indicates that the card requested an online authorization and the transaction was not completed.
Secondary Application Currency Code	Designates a secondary application currency that is converted to the application currency and used for certain velocity checks.
Static Data Authentication Failure Indicator	Indicates that SDA failed during the current or a previous transaction.
Upper Consecutive Offline Limit (“9F59”)	A Visa proprietary data element that is the maximum number of consecutive offline transactions that can be conducted before a transaction must be declined offline if it cannot be sent online.

The card data elements described in Table 13–2 are used by the card during Completion and included in the GENERATE AC command response which the card returns to the terminal.

Table 13–2: GENERATE AC Command Response

Data Element	Description
Cryptogram Information Data	Contains indicators for • The type of cryptogram: – An Application Authentication Cryptogram (AAC) for a decline – A Transaction Certificate (TC) for an approval – An Authorization Request Cryptogram (ARQC) when online processing is requested (first GENERATE AC only) • Other status information including Service Not Allowed
Application Transaction Counter (ATC)	A counter of the number of transactions initiated since the application was put on the card.
Application Cryptogram (AC)	The value of the cryptogram. If the transaction was eligible for Combined DDA/AC Generation and the Cryptogram Information Data shows that the cryptogram is an ARQC or TC, the Application Cryptogram and other data are within an RSA signature
Issuer Application Data • Card Verification Results (CVR)	Contains proprietary application data for transmission to the Issuer. This includes the CVR. • A Visa proprietary data element containing indicators which are set based upon the results of offline processing for current and previous transactions.

The card data elements described in Table 13–3 are used by the terminal during Completion.

Table 13–3: Completion—Card Data Used by Terminal

Data Element	Description
CDOL2	A list of tags and lengths of the terminal data elements that the terminal should include in the second GENERATE AC command.In addition to the tags for data used in the cryptogram algorithm, the tags for the following data elements must be included in the CDOL2 for Completion functions: • Amount, Authorized (if velocity checks using amounts are supported) • Authorization Response Code • Terminal Verification Results (TVR) • Transaction Currency Code (if checks requiring currency code supported) • Terminal Country Code (if checks requiring country code supported) The tags and lengths for some of these data elements may already be included in the CDOL2 as part of the terminal data used for the cryptogram generation. If so, it is not necessary to repeat them.

13.2 Terminal Data

The card uses the terminal data elements described in Table 13–4 for Completion. Appendix A, Card and Issuer Data Element Tables, contains a detailed description of these elements and their usage.

Table 13–4: Completion—Terminal Data (1 of 2)

Data Element	Description
Amount, Authorized	The amount of the current transaction
Authorization Response Code	Provided to the card to indicate the disposition of the transaction • Y1 = Offline approved • Z1 = Offline declined • Y3 = Unable to go online (offline approved) • Z3 = Unable to go online (offline declined)
Terminal Verification Results (TVR)	Used to record offline processing results, such as SDA failure or floor limit exceeded

Table 13–4: Completion—Terminal Data (2 of 2)

Data Element	Description
Terminal Country Code	Indicates the country where the terminal is located
Transaction Currency Code	Indicates the currency code of the transaction

13.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command

The terminal issues a second GENERATE AC command to the card to request the second Application Cryptogram.

The GENERATE AC command contains the terminal data elements specified by the card in the CDOL2, a data element that was received by the terminal during Read Application Data. This CDOL2 data includes the Authorization Response Code specified by the issuer in the online response or by the terminal if an online authorization did not complete.

The P1 parameter in the command indicates the type of cryptogram being requested by the terminal as shown in the *EMV 4.0, Book 3*, Table I-12.

The GENERATE AC response includes the Cryptogram Information Data indicating the card's authorization decision, the Application Transaction Counter, the Application Cryptogram, and Issuer Discretionary Data with the CVR indicating processing results.

13.4 Completion Processing Overview

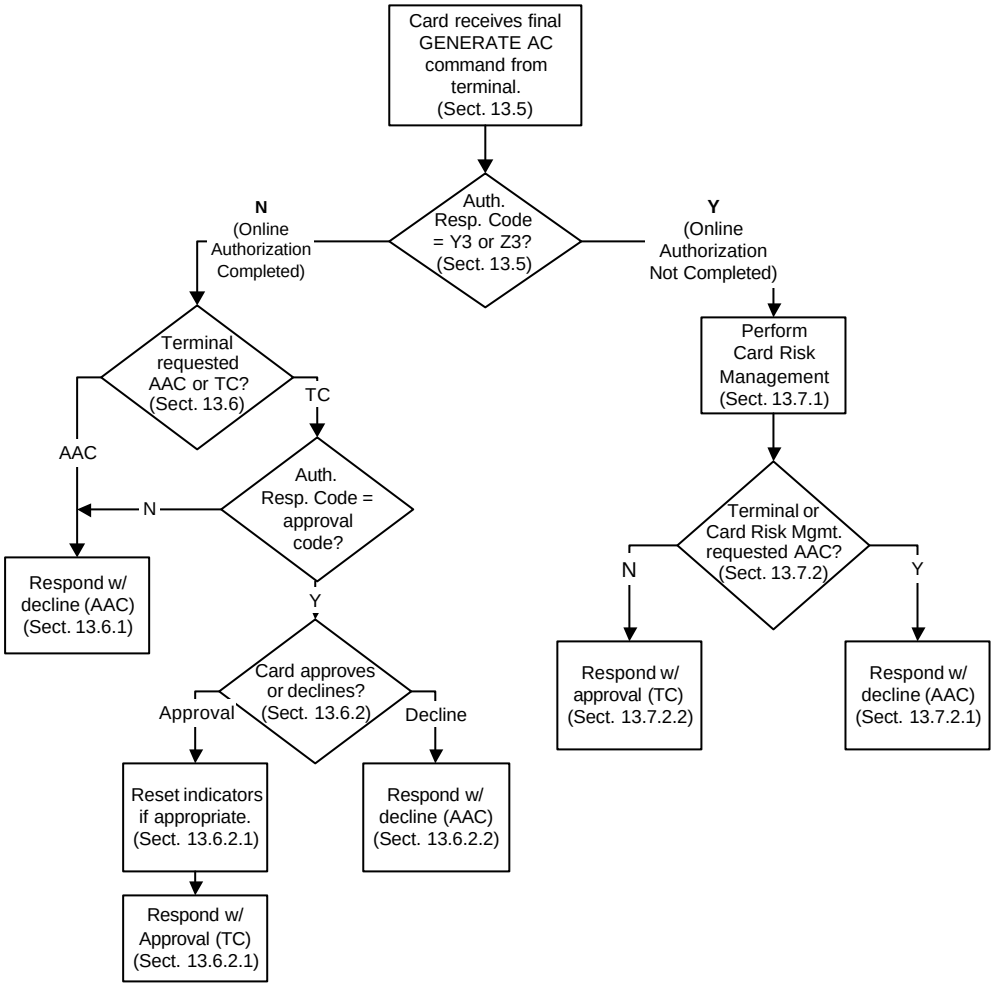
The card only performs Completion processing when the card requested an online authorization during Card Action Analysis.

At the end of Card Action Analysis, the card may have:

- Requested an offline approval or decline. For these transactions, card processing is complete with Card Action Analysis. The card performs no Completion processing.
- Requested an online authorization. The card performs Completion processing for these transactions.

Figure 13–1 shows an overview of Completion processing and the sections of this chapter where each step of processing is described.

Figure 13–1: Completion Processing Flow



13.5 Receive GENERATE AC Command

Completion processing for the card occurs when the card receives the second GENERATE AC command from the terminal. The type of Authorization Response Code in this command determines which path the Completion processing follows:

- An Authorization Response Code other than Y3 or Z3 in the second GENERATE AC command means that the online authorization completed and the terminal received a response from the issuer during Online Processing. The processing of these transactions is described in Section 13.6 Transaction Authorized Online.
- An Authorization Response Code of Y3 or Z3 means that an online authorization was requested but not completed during Online Processing. Either the terminal did not support online processing or a response from the issuer was not received. The processing of these transactions is described in Section 13.7 Online Processing Requested, Online Authorization Not Completed.

13.6 Transaction Authorized Online

When the transaction was authorized online (Authorization Response Code not Y3 or Z3), the card does the following:

- If Issuer Authentication was performed, verifies the Authorization Response Code received in the EXTERNAL AUTHENTICATE command:
  - An Authorization Response Code of 00, 10, or 11 indicates an issuer approval.
  - An Authorization Response Code of 01 or 02 indicates an issuer referral.
  - An Authorization Response Code other than one listed above indicates an issuer decline. These transactions should be processed as though the terminal had requested a decline.
- Checks the P1 parameter of the second GENERATE AC command:
  - If P1 indicates a TC (approval cryptogram) and, if verified above, the Authorization Response Code indicates an issuer approval or referral, approval processing as described in Section 13.6.2 TC (Approval) Requested After Online Authorization is performed.
  - If P1 indicates an AAC (decline cryptogram) or, if verified above, the Authorization Response Code indicates a decline, decline processing as described in the following section is performed.

13.6.1 AAC (Decline) Requested After Online Authorization

When the card receives a request for an AAC in the second GENERATE AC command or the Authorization Response Code shows an issuer decline, the card shall return an AAC. Prior to responding to the terminal with an AAC, the card shall:

- Set the bits in the Card Verification Results (CVR) to indicate that an AAC is returned in the second GENERATE AC response
- If Issuer Authentication was not performed but Issuer Authentication is supported (as shown by the AIP), set the Issuer Authentication not Performed After Online Authorization bit to "1" in the CVR
- If Issuer Authentication was not performed but Issuer Authentication is mandatory (as shown by the Issuer Authentication Indicator), set the Issuer Authentication Failure Indicator to "1"
- If Issuer Authentication is either (1) not supported, (2) optional and not performed, or (3) performed and successful, reset the following indicators to zero:
  - Online Authorization Indicator
  - Static Data Authentication Failure Indicator
  - Dynamic Data Authentication Failure Indicator
  - Issuer Script Command Counter
  - Issuer Script Failure Indicator
- Not update or reset the following:
  - Last Online ATC Register
  - Cumulative Total Transaction Amount
  - Cumulative Total Transaction Amount (Dual Currency)
  - Consecutive Transaction Counter (International)
  - Consecutive Transaction Counter (International—Country)
- Generate the Application Cryptogram as described in Appendix D, Authentication Keys and Algorithms
- Set the Cryptogram Information Data to an AAC
- Return the second GENERATE AC response to the terminal

13.6.2 TC (Approval) Requested After Online Authorization

When the card receives a request for a TC in the second GENERATE AC command and, if checked, the Authorization Response Code indicates an issuer approval or referral, the card performs the following:

- If Issuer Authentication was not performed but Issuer Authentication is supported (as shown by the AIP), set the Issuer Authentication not Performed After Online Authorization bit to "1" in the CVR.

The card may respond with either an approval or a decline response based on the results of card settings for Issuer Authentication.

- **Card Approves**—If *any* of the following conditions are true, the card approves the transaction:
  - Issuer Authentication was successful
  - Issuer Authentication is not supported (as shown in the AIP (Application Interchange Profile))
  - Issuer Authentication is optional (as shown in the Issuer Authentication Indicator) and was not performed
  - Issuer Authentication failed, and the ADA bit for If Issuer Authentication Performed and Failed, Decline Transaction is set to "0"
  - Issuer Authentication is mandatory (as shown in the Issuer Authentication Indicator) and not performed, and the ADA bit for If Issuer Authentication is Mandatory and no ARPC Received, Decline Transaction is set to "0"

Processing for card approved transaction continues with Section 13.6.2.1 Card Approves Transaction After TC (Approval) Requested.

- **Card Declines**—If *any* of the following conditions are true, the card declines the transaction:
  - Issuer Authentication failed and the ADA bit for If Issuer Authentication Performed and Failed, Decline Transaction is set to "1"
  - Issuer Authentication is mandatory (as shown in the Issuer Authentication Indicator) and not performed, and the ADA bit for If Issuer Authentication is Mandatory and No ARPC Received, Decline Transaction is set to "1"

Processing for card declined transactions continues with Section 13.6.2.2 Card Declines Transaction After TC (Approval) Requested.

13.6.2.1 Card Approves Transaction After TC (Approval) Requested

When the card approves the transaction, it shall:

1. Set the bits in the CVR to indicate that a TC is being returned in the second GENERATE AC response.
2. Set the type of cryptogram in the Cryptogram Information Data in the GENERATE AC response to a TC.
3. Reset counters and indicators based upon Issuer Authentication results and requirements as steps 3a and 3b:
   a. If Issuer Authentication either (1) failed or (2) was mandatory (as shown in Issuer Authentication Indicator) and not performed, the card shall:
      - Not update or reset the following:
        - Last Online ATC Register
        - Cumulative Total Transaction Amount
        - Cumulative Total Transaction Amount (Dual Currency)
        - Consecutive Transaction Counter (International)
        - Consecutive Transaction Counter (International—Country)
        - Online Authorization Indicator
        - Static Data Authentication Failure Indicator
        - Dynamic Data Authentication Failure Indicator
        - Issuer Script Command Counter
        - Issuer Script Failure Indicator
      - If Issuer Authentication is mandatory and was not performed:
        - Set the Issuer Authentication Failure Indicator to “1”.
        - Set Issuer Authentication Not Performed After Online Authorization in the CVR to “1”.

b. If Issuer Authentication was either (1) successful, (2) optional and was not performed, or (3) is not supported, the card shall:

- If Issuer Authentication is supported (as shown by the AIP) and the card did not receive an EXTERNAL AUTHENTICATE command, set the Issuer Authentication not Performed After Online Authorization bit in the CVR to "1".
- Reset the following indicators and counters to zero:
  - Online Authorization Indicator
  - Static Data Authentication Failure Indicator
  - Dynamic Data Authentication Failure Indicator
  - Issuer Script Command Counter
  - Issuer Script Failure Indicator
  - Cumulative Total Transaction Amount
  - Cumulative Total Transaction Amount (Dual Currency)
  - Consecutive Transaction Counter (International)
  - Consecutive Transaction Counter (International—Country)
- Update the Last Online ATC Register to the current value of the ATC.

4. Generate the Application Cryptogram as described in Appendix D, Authentication Keys and Algorithms.
5. Return the second GENERATE AC response to the terminal.

13.6.2.2 Card Declines Transaction After TC (Approval) Requested

When the card has declined a transaction where an approval was requested, the card shall:

- Set the bits in the CVR to indicate that an AAC is being returned in the second GENERATE AC response.
- If Issuer Authentication is supported and mandatory, set Issuer Authentication Failure Indicator to "1".
- Set the type of cryptogram in the Cryptogram Information Data in the GENERATE AC response to an AAC.

- If the ADA bit for If Transaction Declined Because Issuer Authentication Failed or Not Performed, Create Advice is set to “1”, set the Advice Required bit to “1” in Cryptogram Information Data.
- Not update or reset the following:
  - Cumulative Total Transaction Amount
  - Cumulative Total Transaction Amount (Dual Currency)
  - Consecutive Transaction Counter (International)
  - Consecutive Transaction Counter (International—Country)
  - Last Online ATC Register
  - Online Authorization Indicator
  - Static Data Authentication Failure Indicator
  - Dynamic Data Authentication Failure Indicator
  - Issuer Script Command Counter
  - Issuer Script Failure Indicator

The card shall:

- Generate the Application Cryptogram as described in Appendix D, Authentication Keys and Algorithms.
- Return the second GENERATE AC response to the terminal.

13.7 Online Processing Requested, Online Authorization Not Completed

When the second GENERATE AC command from the terminal contains an Authorization Response Code indicating that online processing was requested but not completed (Y3 or Z3), the card shall:

- Perform the optional card risk management checks which are supported (Section 13.7.1 Card Risk Management).
- Respond back to the terminal (Section 13.7.2 Card Response After Unable to Go Online).

13.7.1 Card Risk Management

Card risk management includes optional checks to determine if the number of offline transactions has exceeded the Upper Consecutive Offline Limit, if the offline amount limit has been exceeded, if the card is a new card, and if the PIN Try Limit was exceeded on a previous transaction.

When the online authorization was not completed, the card shall perform all of the supported card risk management checks even if the terminal requested a decline (AAC) in the second GENERATE AC command or a previous card risk management check results in a decline. Since the card performs all checks, the order in which the checks are performed need not conform to the order described below.

13.7.1.1 Velocity Checking for Total Consecutive Offline Transactions (Upper Limit)

This check is optional for the card and determines if the limit set for the maximum number of total consecutive offline transactions has been exceeded.

The card shall perform this check if the Last Online ATC Register is present in the card and the Visa proprietary Upper Consecutive Offline Limit (tag “9F59”) are present in an internal file.

If the difference between the ATC and the Last Online ATC Register is greater than the Upper Consecutive Offline Limit, velocity checking limits have been exceeded. The card shall:

- Set the Exceeded Velocity Checking Counters bit to “1” in the CVR.
- Set the Offline Decline Requested by Card Indicator to “1” to indicate that an AAC should be returned after completion of card risk management.

13.7.1.2 New Card

This check is optional for the card and determines if the card has previously been approved online.

The card shall perform this check if the Last Online ATC Register is present in the card. If the Application Default Action (ADA) is not present, a default value of zeros is used.

If the Last Online ATC Register is zero, the card shall:

- Set the New Card bit to “1” in the CVR.
- If the ADA bit for If New Card, Decline if Unable to Transmit Online is set to “1”, the card sets the Offline Decline Requested by Card Indicator to “1” to indicate that an AAC should be returned after completion of card risk management.

13.7.1.3 PIN Try Limit Exceeded

This optional check determines if the PIN Try Limit has been exceeded on a previous transaction.

If the Application Default Action (ADA) is not present, a default value of zeros is used.

If Offline PIN verification is supported by the card and the card has not received a VERIFY command from the terminal during the current transaction, the card shall:

- If the PIN Try Counter is zero and the ADA bit for If PIN Try Limit Exceeded on Previous Transaction, Decline If Unable to Transmit Transaction Online (Byte 2 bit 5) is set to "1":
  - Set Offline Decline Requested by Card Indicator to "1" to indicate that an AAC should be returned after completion of card risk management.
  - Set the PIN Try Limit Exceeded bit in the CVR.

13.7.1.4 Velocity Checking for Transaction Amount (Upper Limit)

This check is optional for the card and determines if the limit set for the maximum cumulative transaction amount for consecutive offline transactions in the primary currency has been exceeded.

The card shall perform this check if the Cumulative Total Transaction Amount and Cumulative Total Transaction Amount Upper Limit are present in an internal file.

If the sum of the Cumulative Total Transaction Amount and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Upper Limit, the card shall:

- Set the Exceeded Velocity Checking Counters bit to "1" in the CVR.
- Set the Offline Decline Requested by Card indicator to "1" to indicate that an AAC should be returned after completion of card risk management.

13.7.1.5 Velocity Checking for Transaction Amount (Dual Currency) (Upper Limit)

This check is optional for the card and determines if the limit set for the maximum cumulative transaction amount for consecutive offline transactions in the primary and secondary currencies has been exceeded.

The card shall perform this check if the Cumulative Total Transaction Amount (Dual Currency) and Cumulative Total Transaction Amount Upper Limit are present in an internal file.

If the sum of the Cumulative Total Transaction Amount (Dual Currency) and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Upper Limit, the card shall:

- Set the Exceeded Velocity Checking Counters bit to "1" in the CVR.
- Set the Offline Decline Requested by Card indicator to "1" to indicate that an AAC should be returned after completion of card risk management.

13.7.2 Card Response After Unable to Go Online

Based upon the cryptogram type requested by the terminal and the results of the card risk management steps, the card responds to the GENERATE AC command issued by the terminal as follows:

The card declines if *either* of the following conditions are true:

- Terminal requested an AAC in the second GENERATE AC
- Card Risk Management has resulted in the Offline Decline Requested by Card Indicator being set to "1"

This decline processing is described in Section 13.7.2.1 Card Declined Transaction After Unable to Go Online.

The card approves if *both* of the following conditions are true:

- Terminal requested a TC in the second GENERATE AC command
- Card Risk Management has not resulted in the Offline Decline Requested by Card Indicator being set to "1"

This approval processing is described in Section 13.7.2.2 Card Approved Transaction After Unable to Go Online.

13.7.2.1 Card Declined Transaction After Unable to Go Online

This section describes the card processing when the card is declining after a request for an online authorization did not complete (Authorization Response Y3 or Z3). The card shall:

- Set the bits in the CVR to indicate:
  - An AAC is being returned in the second GENERATE AC response.
  - The terminal was "Unable to Go Online".
- If the TVR bit for Offline Static Data Authentication Failed is set to "1", set the Static Data Authentication Failure Indicator to "1".
- If the TVR bit for Offline Dynamic Data Authentication Failed is set to "1", set the Dynamic Data Authentication Failure Indicator to "1".

- If the TVR bit for Combined DDA/AC Generation failed is set to “1”, set the Dynamic Data Authentication Failure Indicator to “1”.
- If the Terminal Country Code is not equal to the Issuer Country Code, increment the Consecutive Transaction Counter (International—Country) by one.
- If the Transaction Currency Code is not equal to the Application Currency Code, increment the Consecutive Transaction Counter (International) by one.
- If the ADA bit for If Transaction Declined Offline, Create Advice equals “1”, set the Advice Required bit to “1” in the Cryptogram Information Data.
- Do not update the Last Online ATC Register.
- Generate an Application Cryptogram as described in Appendix D, Authentication Keys and Algorithms.
- Set the Cryptogram Information Data to an AAC.
- Return the second GENERATE AC response to the terminal.

13.7.2.2 Card Approved Transaction After Unable to Go Online

This section describes the card processing when the card is approving after a request for an online authorization did not complete (Authorization Response Y3 or Z3). The card shall:

- Set bits in the CVR to indicate:
  - A TC is returned in the second GENERATE AC response.
  - The terminal was “Unable to go online”.
- If the Terminal Country Code is not equal to the Issuer Country Code, increment the Consecutive Transaction Counter (International—Country) by one.
- If the Transaction Currency Code is equal to the Application Currency Code:
  - Increment the Cumulative Total Transaction Amount by the Amount, Authorized.
  - Increment the Cumulative Total Transaction Amount (Dual Currency) by the Amount, Authorized.
- If the Transaction Currency Code is not equal to the Application Currency Code, increment the Consecutive Transaction Counter (International) by one.

- If the Transaction Currency Code is equal to the Secondary Application Currency Code, increment the Cumulative Total Transaction Amount (Dual Currency) by Amount, Authorized converted to the Application Currency.
- Do not update the Last Online ATC Register.
- Generate an Application Cryptogram as described in Appendix D, Authentication Keys and Algorithms.
- Set the Cryptogram Information Data to a TC.
- Return the second GENERATE AC response to the terminal.

13.8 Completion Processing Transaction Flow

Table 13–2 shows how a card could perform Completion processing.

Figure 13–2: Transaction Flow (1 of 5)

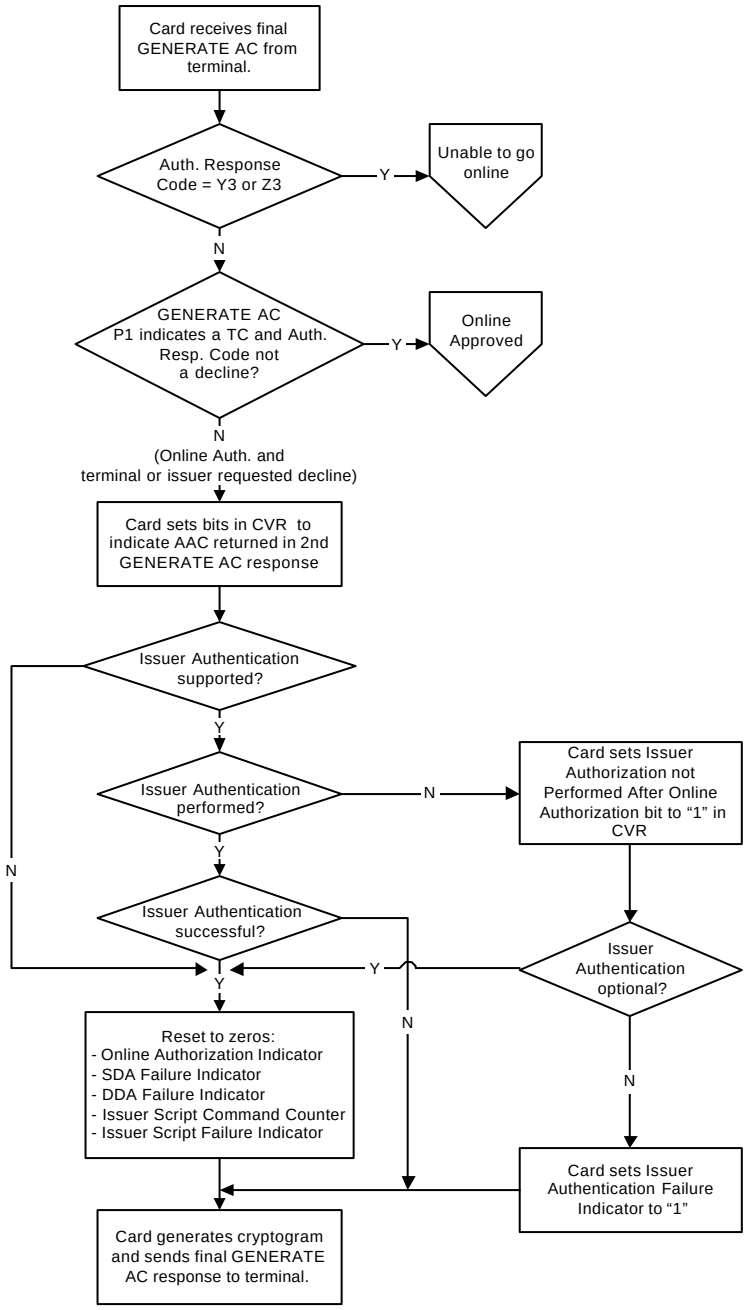


Figure 13–3: Transaction Flow (2 of 5)

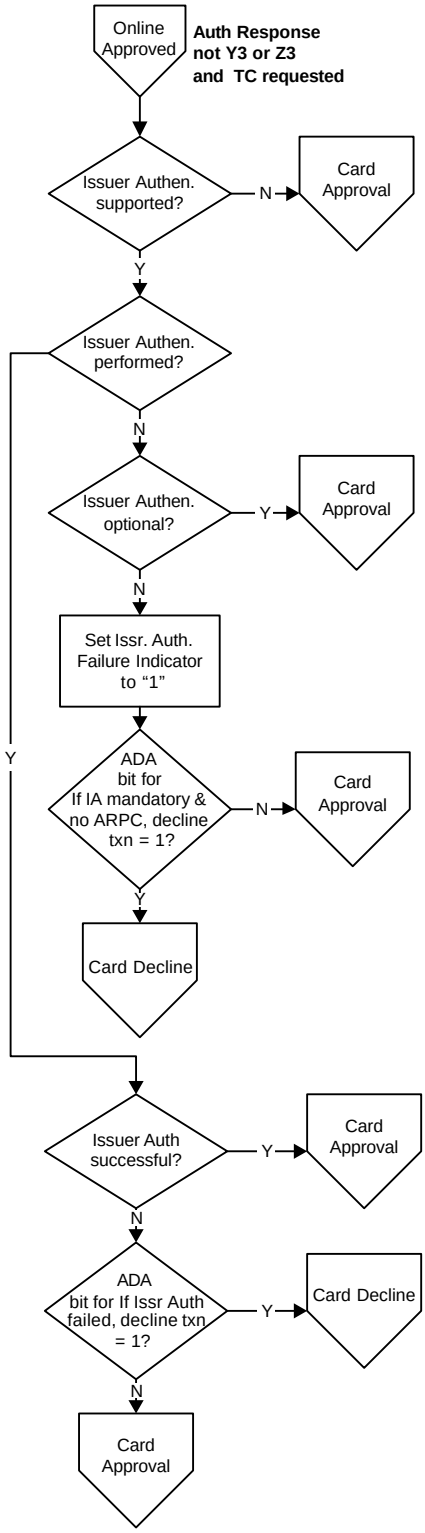


Figure 13–4: Transaction Flow (3 of 5)

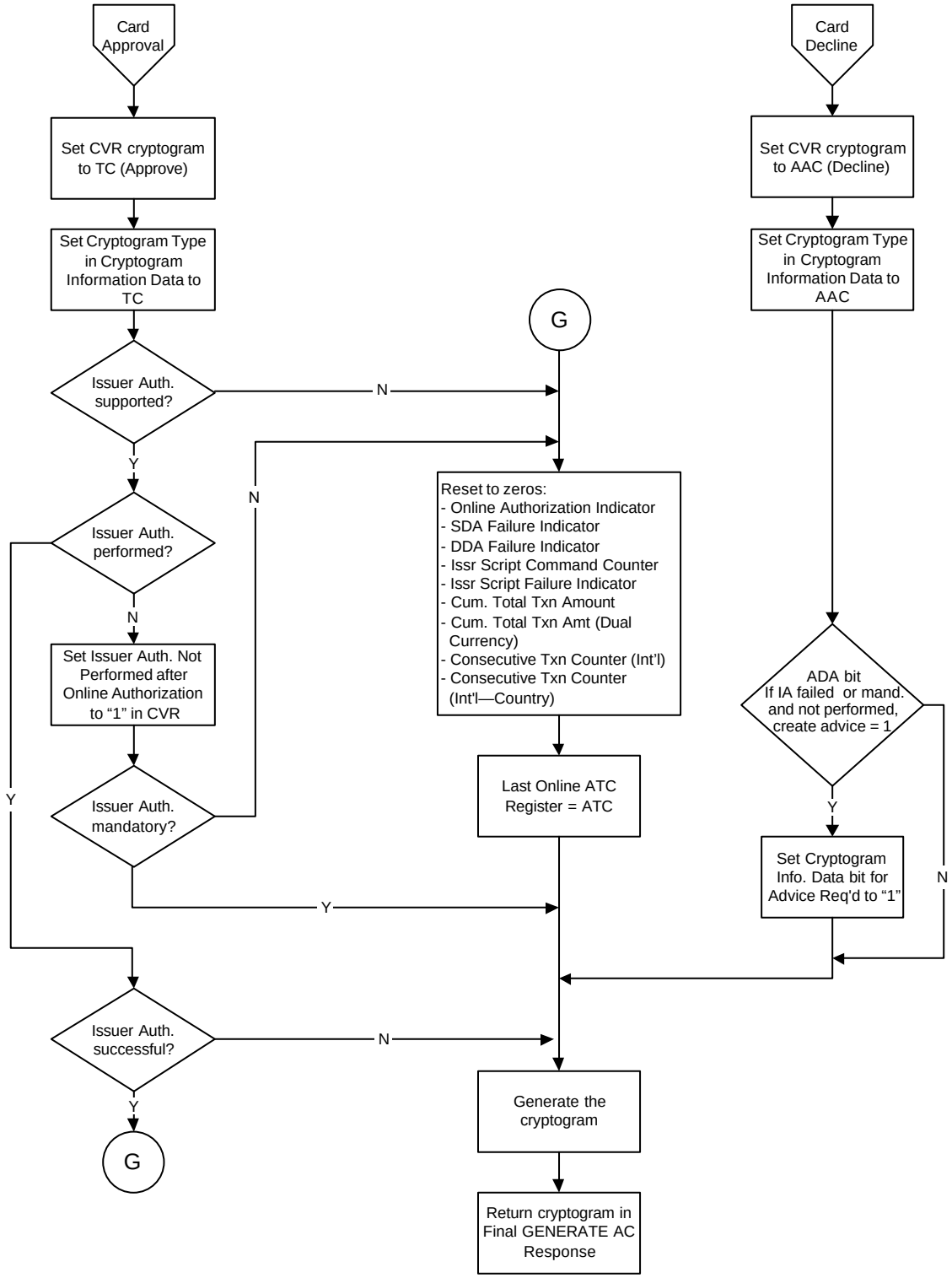
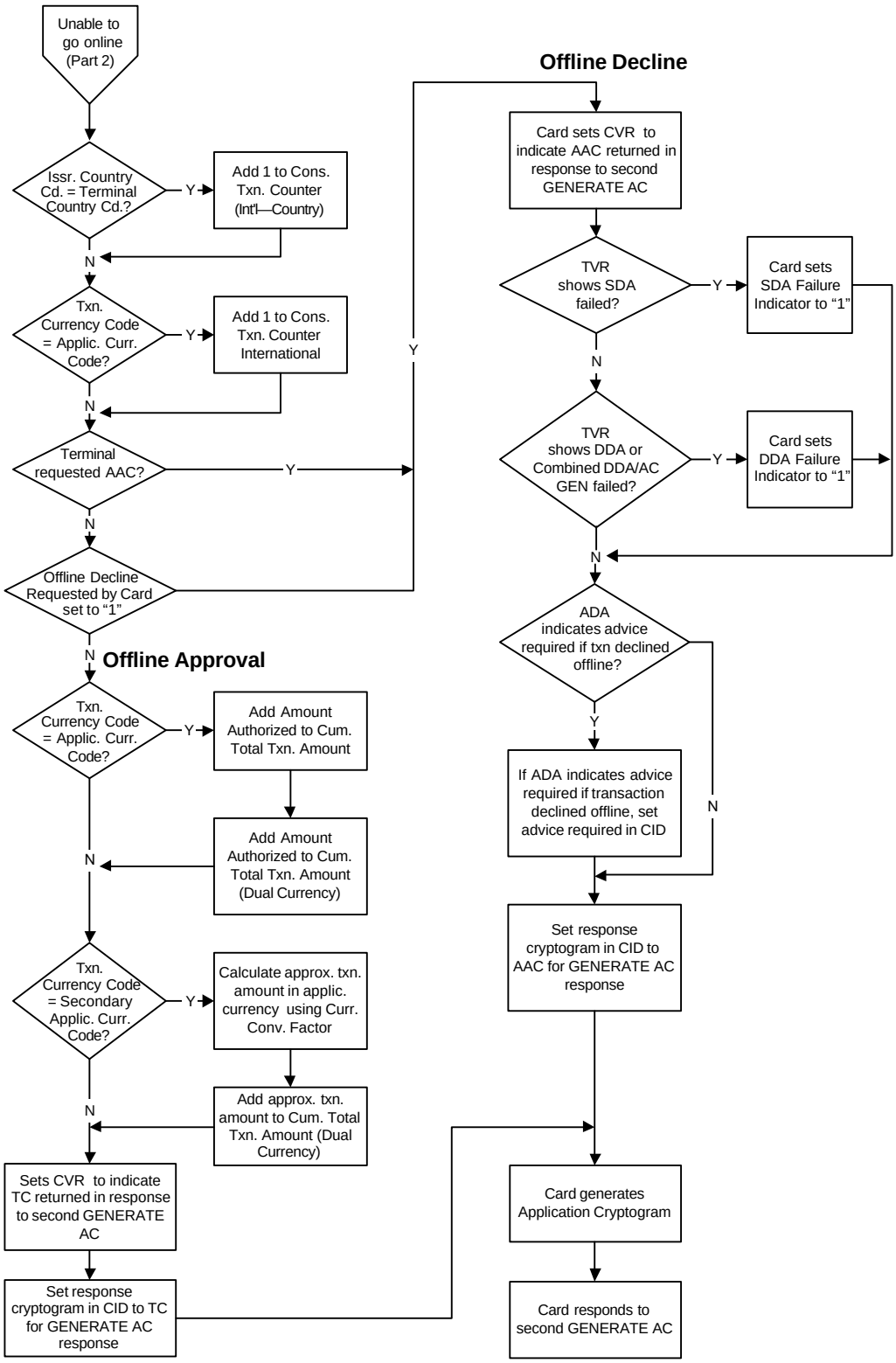


Figure 13–5: Transaction Flow (4 of 5)

Figure 13–6: Transaction Flow (5 of 5)



13.9 Prior Related Processing

Card Action Analysis

The card requests an online authorization, an offline approval, or an offline decline. During Completion, the terminal only issues a second GENERATE AC command to the card for transactions where the card requested an online authorization. The card does no Completion processing for transactions where the card requested an offline approval or offline decline during Card Action Analysis.

Online Processing

If the card receives an EXTERNAL AUTHENTICATE command from the terminal, the ARPC in that command is validated and indicators are set for Issuer Authentication performed and passed or for Issuer Authentication performed and failed.

13.10 Subsequent Related Processing

Card Action Analysis (Subsequent Transactions)

On following transactions, the card uses indicators and counters set during Completion in its processing decisions.

Issuer-to-Card Script Processing 14

Issuer-to-Card Script Processing enables issuers to change personalized data on cards without reissuance. With this function, the issuer transmits commands in issuer scripts contained in the authorization response message. The terminal passes these commands to the card where they are executed if security requirements are satisfied.

Issuer-to-Card Script Processing shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Section 2, and *Book 4*, Section 2.3.9.

Commands are supported for:

- Updating card parameters
- Blocking or unblocking the application
- Blocking the card
- Resetting the PIN Try Counter
- Changing the offline PIN

Issuer-to-Card Script Processing limits credit and fraud exposure by allowing blocking of overspent and stolen cards. Card parameters can be modified to correspond to changing cardholder circumstances without reissuing the card.

This chapter is organized in the following manner:

14.1 Key Management for Issuer Script Processing

14.2 Card Data

14.3 Terminal Data

14.4 Authorization Response Data

14.5 Commands

14.6 Processing

14.7 Prior Related Processing

14.8 Subsequent Related Processing

14.1 Key Management for Issuer Script Processing

Issuer-to-Card Script Processing uses unique cryptographic keys to provide message authentication and to support confidentiality of private script data such as PINs. These keys shall be unique to the specific cryptographic function and shall not be used for any other purpose. The card and the issuer shall be capable of selecting the appropriate cryptographic key based upon the cryptographic function being performed.

All data required to perform the Issuer Script commands and their associated tasks (for example, Message Authentication Code (MAC) generation, PIN encipherment, key derivation) shall be available to both the issuer and the card operating system.

Message Authentication Keys

The following keys are used to authenticate that the script came from the valid issuer and ensure that the script has not been modified:

- **Master Message Authentication Code Key (MAC MDK)**—A double-length DES key generated by the issuer and used by the issuer's personalization and authorization systems for secure messaging. The MAC MDK is used to generate a card-unique MAC key (MAC UDK) that is personalized on the card. During the processing of online transactions, the issuer's host authorization system uses the MAC MDK to generate the card level MAC UDK that is used to generate the MAC Session Key. This MAC Session Key is used to calculate the MAC value for each script command in the online response. The issuer shall support a MAC MDK if the issuer supports processing of commands that require secure messaging, such as an Issuer Script Command.
- **Unique Message Authentication Code Key (MAC UDK)**—A card-unique key used for secure messaging. It is generated prior to card personalization using the MAC MDK, the PAN, and the PAN Sequence Number. During the transaction, the card uses the MAC UDK to generate a transaction-unique MAC Session Key. A MAC UDK shall be present on the card if the card supports processing of a command that requires secure messaging, such as an Issuer Script Command.

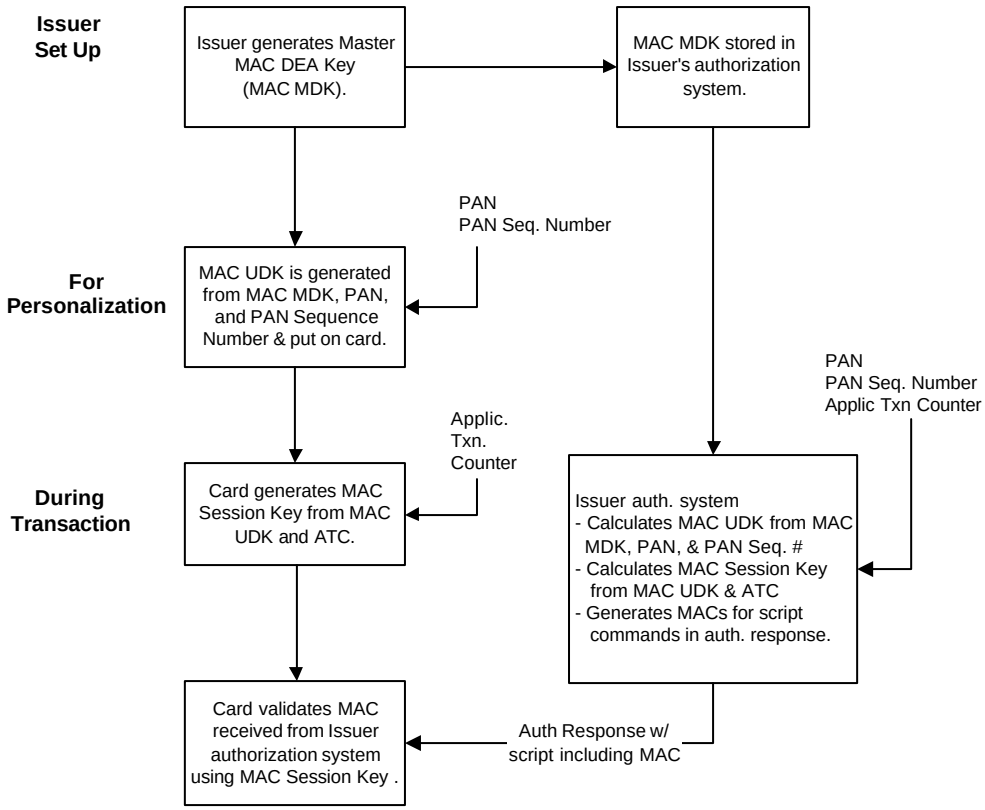
  The MAC UDK is a double-length DES key comprised of MAC Key A and MAC Key B. The method for generating the MAC UDK is the same method used for the Unique DEA key and is described in Appendix D, Authentication Keys and Algorithms.
- **MAC Session Key**—A transaction-unique key which is generated by the issuer host during online transactions and is used to calculate a MAC value which is included in the Issuer Script. When the card receives the script, it generates the MAC Session Key from the MAC UDK and uses it to recalculate the MAC value for comparison to the MAC in the script.

Validation of the MAC proves that the command has not been altered (message integrity) and that it was sent by the valid issuer (message authentication).

The MAC Session Key is a double-length DES key. At transaction time, the issuer host generates the MAC UDK from the MAC MDK, the PAN, and the PAN Sequence Number. It uses this MAC UDK and the Application Transaction Counter (ATC) to generate the MAC Session Key. In the card, the MAC Session Key is generated from the MAC UDK and the ATC. The method for generating the MAC Session Key is described in Appendix B, Secure Messaging.

Figure 14–1 shows how these MAC keys are generated and used.

Figure 14–1: Generation and Use of MAC Keys



Data Encipherment Keys

The following Data Encipherment Keys are used to encrypt and decrypt confidential data such as PINs in issuer scripts:

- **Master Data Encipherment DEA Key (ENC MDK)**—A double-length DES key generated by the issuer and used by the issuer's personalization and authorization systems to provide privacy for confidential script data. The issuer uses the ENC MDK, the PAN, and the PAN Sequence Number to generate a card's Unique Data Encipherment DEA Key (ENC UDK) that is personalized on the card. During the transaction, the issuer's online authorization system uses the ENC MDK to generate the card level ENC UDK that is used to generate the Data Encipherment Session Key. The Data Encipherment Session Key is used to encrypt confidential data in script commands. The issuer shall support an ENC MDK if its cards support Issuer Script processing with confidential data such as offline PINs.
- **Unique Data Encipherment DEA Key (ENC UDK)**—A card-unique key generated using the Master Data Encipherment DEA Key (ENC MDK), the PAN, and the PAN Sequence Number. During the transaction, the card uses the ENC UDK to generate the Data Encipherment Session Key that decrypts the enciphered script data.

  The ENC UDK shall be present if *both* of the following conditions exist:

  – The card supports Issuer Script processing

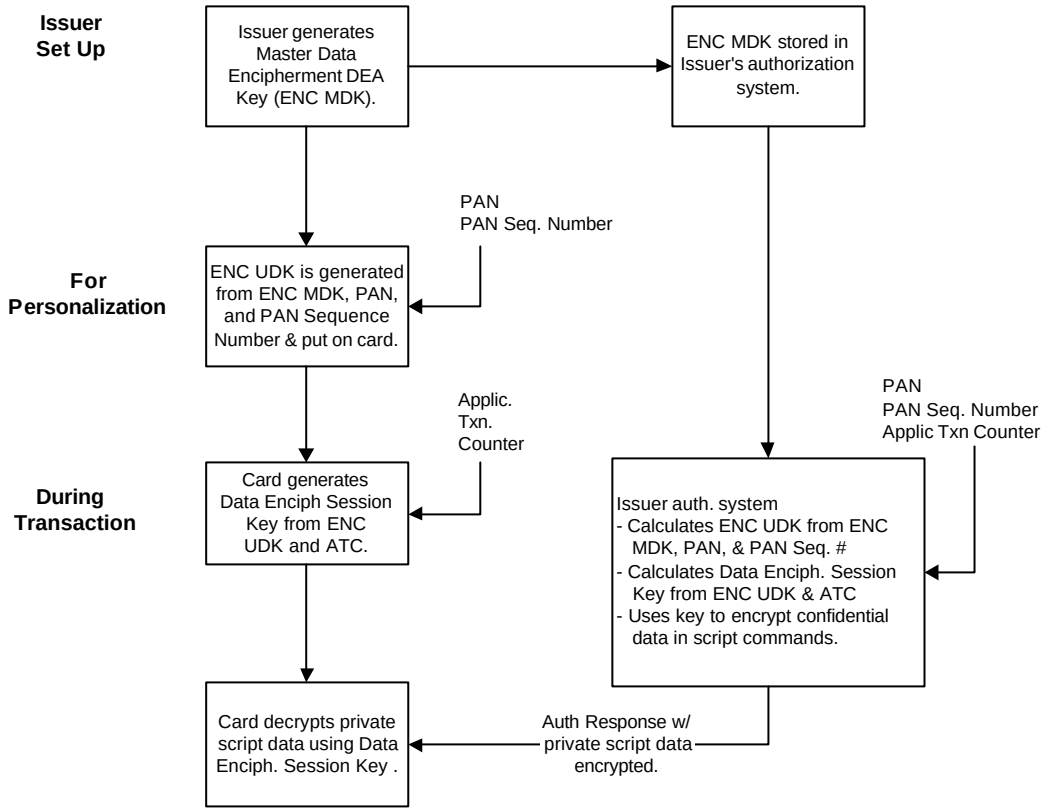
  – Enciphered data such as an offline PIN may be contained in an Issuer Script command

  The Data Encipherment DEA Key (ENC UDK) is a double-length DES key comprised of the Data Encipherment DEA Key A and Key B. The method for generating the ENC UDK is the same method used for the Unique DEA key and is described in Appendix D, Authentication Keys and Algorithms.
- **Data Encipherment Session Key**—A transaction-unique key which is generated by the issuer host during online transactions and used to encrypt confidential data in issuer scripts. Encryption of the data keeps the data private during transmission. The card generates this Data Encipherment Session Key from the ENC UDK when it receives the script command containing enciphered data. The card uses the session key to decrypt the enciphered data.

The Data Encipherment Session Key is a double-length DES key. At transaction time, the issuer host generates the ENC UDK from the ENC MDK, the PAN, and the PAN Sequence Number. It then generates the Data Encipherment Session Key from this ENC UDK and the ATC. In the card, the Data Encipherment Session Key is generated from the ENC UDK and the ATC. This method for generating the Data Encipherment Session Key is described in detail in Appendix B, Secure Messaging.

Figure 14–2 shows how these data encipherment keys are generated and used.

Figure 14–2: Generation and Use of Data Encipherment Keys



14.2 Card Data

The card counters and indicators described in Table 14–1 are used in Issuer-to-Card Script Processing. For a detailed description of these data elements and their usage, see Appendix A, Card and Issuer Data Element Tables.

Table 14–1: Issuer-to-Card Script Processing—Card Data

Data Element	Description
Application Transaction Counter (ATC)	A card counter that is incremented with each transaction. It is used in the generation of session keys used in script processing.
Card Verification Results (CVR)	In subsequent transactions the Card Action Analysis function fills in the following CVR subfields: • Number of Issuer Script Commands Received After the Final GENERATE APPLICATION CRYPTOGRAM (AC) Command Containing Secure Messaging Processed on Last Transaction—Contains value from Issuer Script Command Counter. • Issuer Script Processing Failed on Last Transaction indicator—Set to “1” if the Issuer Script Failure indicator is set to “1”.
Issuer Script Command Counter	The Issuer Script Command Counter is used by the card to count each command containing secure messaging that was received after the second GENERATE AC command. On subsequent transactions this counter may be reset during Completion.
Issuer Script Failure Indicator	The card shall set the Issuer Script Failure indicator to “1” if one of the following error conditions occurs during card processing of a command received after the Second GENERATE AC command: • Secure messaging failed (Calculated MAC not equal to MAC in command) • Secure messaging passed but processing of the command failed • Secure messaging is required to perform the command but was not present Failure of script processing for a command that does not require secure messaging shall not impact this indicator. On subsequent transactions this indicator may be reset during Completion.

14.3 Terminal Data

The terminal data described in Table 14–2 is used in Issuer-to-Card Script Processing. For a detailed description of these data elements and their usage, refer to the *Visa Integrated Circuit Card Terminal Specification*, Appendix A, Card and Issuer Data Element Tables.

Table 14–2: Issuer-to-Card Script Processing—Terminal Data

Data Element	Description
Issuer Script Results	Issuer Script Results contains the results of Issuer Script processing and is included in the clearing message and the next online authorization
Terminal Verification Results (TVR)	The TVR contains two script related indicators: • Issuer Script Failed Before Final GENERATE AC command • Issuer Script Failed After Final GENERATE AC command
Transaction Status Information (TSI)	The TSI contains a flag indicating that Issuer Script Processing was performed

14.4 Authorization Response Data

The issuer includes the Issuer Script data described in Table 14–3 in the authorization response if Issuer-to-Card Script Processing is to occur.

Table 14–3: Issuer-to-Card Script Processing—Online Response Data

Data Element	Description
Issuer Script Template	Only Issuer Script Template 2 is supported for cards in this version of the Visa Integrated Circuit Card Specification. Tag “72” identifies Issuer Script Template 2 and contains proprietary issuer data for transmission to the card after the second GENERATE APPLICATION CRYPTOGRAM (AC) command. Tag “71” is not used in this version of *Visa Integrated Circuit Card Specification*. Tag “71” identifies Issuer Script Template 1 containing proprietary issuer data for transmission to the card before the second GENERATE AC command.
Issuer Script Identifier	The Issuer Script Identifier is a number used by the issuer to uniquely identify the issuer script
Issuer Script Commands	Each Issuer Script command in the script is in BER-TLV format with a tag of “86”

14.5 Commands

The functions that may be performed using Issuer-to-Card Script Processing are listed below. The Issuer Script Commands that are recommended for use to support these functions are described in detail in either the *EMV 4.0, Book 3*, Section 2.5, and in Appendix C, Commands for Financial Transactions, of this document.

All commands apply to the currently selected application with the exception of the CARD BLOCK command.

APPLICATION BLOCK

Application blocking may be performed if the issuer determines that the application in use should be invalidated. The blocked application may subsequently be unblocked by the issuer.

The blocking of an application through the use of the APPLICATION BLOCK command shall mean that the file status indicator associated with the application is set to reflect that the application has been blocked. Internal access to all the application's data shall be available even when the application is blocked. When an application has been blocked, the card shall always return an Application Authentication Cryptogram (AAC) in the response to a GENERATE APPLICATION CRYPTOGRAM (AC) command.

If the application is blocked during the processing of a transaction, the card and terminal shall continue to process the transaction through Completion. During any subsequent Application Selection, the card shall not allow the blocked application to be available for application selection to perform a financial transaction. (It is possible for the terminal to select an application that was blocked in order to unblock the application. However, if this occurs, the card is required to return an AAC in response to a GENERATE AC command.)

During personalization, multiple AIDs may be linked for blocking. This might be done when an account is represented by multiple AIDs. Blocking a single AID shall block all AIDs that were linked to that AID for blocking. One method of linking AIDs for blocking is shown in the Common Personalization for VSDC document.

APPLICATION UNBLOCK

Unblocking the application reverses the APPLICATION BLOCK status. In this version of VIS, unblocking of an application should occur only at a special device as designated by the issuer.

Since unblocking the application is performed at a special device, the transaction processing flow need not comply with the normal processing rules for an authorization or financial transaction. The device shall be able to transmit the transaction online after the card has returned an Application Authentication Cryptogram (AAC) in the response to the first GENERATE APPLICATION CRYPTOGRAM (AC) command. Issuer Authentication need not be performed even if the card supports Issuer Authentication. It is not necessary for card risk management or terminal risk management to be performed. It is not necessary for a second GENERATE AC command to be generated. (If for any reason the card is unblocked prior to the second GENERATE AC command being issued, the device shall treat the cryptogram returned in the response as an AAC.)

During personalization, multiple AIDs may be linked for unblocking. This might be done when an account is represented by multiple AIDs. Unblocking a single AID shall unblock all AIDs that were linked to that AID for unblocking. One method of linking AIDs for unblocking is shown in the *Common Personalization for VSDC* document.

CARD BLOCK

The CARD BLOCK command is a post-issuance command that permanently disables all applications on the card.

The CARD BLOCK command invalidates all applications on the card and effectively shuts the card down, although the card life cycle data shall be retrievable through the use of the GET DATA command as described in Appendix C, Commands for Financial Transactions. Except when a card is blocked, the Payment System Environment (PSE) shall never be invalidated and shall always remains accessible.

If the card is blocked during the processing of a transaction, the card and terminal shall continue to process the transaction through to Completion. A blocked card shall never be unblocked using an Issuer Script Command or any other command; therefore, the card is essentially disabled. If the card is blocked, the PSE shall be invalidated. Therefore, the card shall respond to a SELECT command with status words indicating “Function not supported” (SW1 SW2 = “6A81”) and shall perform no further actions. The card shall not allow any other form of application selection such as implicit selection.

Card blocking may be performed if the issuer determines that any future use of the card is to be prevented. Card blocking is usually performed only if the card has been reported as lost or stolen, since none of the applications in the card can be unblocked subsequent to card blocking.

Visa recommends that all cards support some means by which the card can be blocked. The support of the CARD BLOCK command in Issuer Script processing is one method by which this may be accomplished.

PIN CHANGE/UNBLOCK

The PIN CHANGE/UNBLOCK command provides the issuer the capability either to unblock the Reference PIN or to simultaneously change and unblock the Reference PIN. The card unblocks the Reference PIN by resetting the PIN Try Counter to the value of the PIN Try Limit.

- Unblocking the PIN

  The PIN Try Counter shall be reset to the PIN Try Limit as a result of a command transmitted by the terminal only if an Issuer Script Command such as the PIN CHANGE/UNBLOCK command is successfully performed during Issuer Script processing.

- Changing the PIN

  If the Reference PIN is being changed, all PIN data shall be enciphered using Data Encryption Algorithm (DEA) in accordance with International Organisation for Standardisation (ISO) 9564. The encipherment method is described in Section 14.6.3 Card Secure Messaging, and in Appendix B.3 Data Confidentiality. Whenever the card's Reference PIN is changed, the card implicitly unblocks the PIN, since the successful completion of the PIN CHANGE/UNBLOCK command automatically resets the PIN Try Counter to the PIN Try Limit.

  Regardless of the method used, PIN change should only be performed within a secure environment controlled by the issuer.

PUT DATA

The PUT DATA command allows specific primitive data objects in the card to be updated. A data object can be updated with this command only if it has a tag associated with it.

In this version of the specification, the following data objects may be updated using the PUT DATA command. A proprietary internal file shall always used for these data elements:

- Upper Consecutive Offline Limit (tag “9F59”)
- Lower Consecutive Offline Limit (tag “9F58”)
- Consecutive Transaction Limit (International)
- Cumulative Total Transaction Amount Limit
- Cumulative Total Transaction Amount Upper Limit
- Cumulative Total Transaction Amount Limit (Dual Currency)
- Consecutive Transaction Limit (International—Country)
- Currency Conversion Factor
- VLP Funds Limit
- VLP Single Transaction Limit

The Upper Consecutive Offline Limit and Lower Consecutive Offline Limit used to support terminal velocity checking (tags “9F14” and “9F23” respectively) are stored in files identified by Short File Identifiers (SFI) 1–10. They are updated in Issuer Script processing using the UPDATE RECORD command, not the PUT DATA command.

UPDATE RECORD

The UPDATE RECORD command is used to update a record in a file with the data provided in the command data field.

The UPDATE RECORD command is required to update the PIN Verification Value (PVV) in the track data to support a PIN change or to update the velocity limits shown previously with the PUT DATA command if these limits are stored in files identified by SFIs 1–10 to support terminal velocity checking.

14.6 Processing

Issuer Scripts are processed in the following manner:

14.6.1 Authorization Response Message

An Issuer Script transmitted in the response message shall always have tag "72" indicating that Issuer Script processing is to be performed after the Second GENERATE AC command. At most one Issuer Script is transmitted in the response message. (In a subsequent version of this specification, issuers may transmit more than one Issuer Script.) A script may contain multiple commands.

The Issuer Script commands defined in the *EMV 4.0, Book 3*, Section 2.5, and in Appendix C of this document, Commands for Financial Transactions, are used to perform the functions described in Section 14.5 Commands.

Any command to update, reset, change, or alter in any way information in the card shall support secure messaging and require that secure messaging must be successfully performed. The recommended method for performing secure messaging is found in Appendix B, Secure Messaging, and Section 14.6.3 Card Secure Messaging.

The originator of an Issuer Script command is assumed to be the card issuer. If an entity other than the issuer originates the commands, the same requirements apply.

14.6.2 Card Script Processing

Since Issuer Script Commands are not identified as such when transmitted to the card, the card is unable to distinguish between an Issuer Script Command and any other command. Therefore, the card shall not reject a command solely because it was received prior to the second GENERATE AC command rather than subsequently.

Section 14.6.5 Resulting Indicators, describes the setting of Visa proprietary indicators relating to Issuer Script processing when an Issuer Script Command is transmitted to the card after the second GENERATE AC command.

14.6.3 Card Secure Messaging

Visa requires that authentication of the issuer using secure messaging shall be successfully performed before processing an Issuer Script Command. Issuer Authentication as described in Chapter 12, Online Processing, need not be performed for script processing.

Secure messaging shall be performed as described in the *EMV 4.0, Book 2*, Section 9. Additional information on secure messaging is contained in Appendix B, Secure Messaging, of this document.

Although secure messaging may be used with a command other than the Issuer Script Commands described in Section 14.5 Commands, this section describes the use of secure messaging in the context of the processing of those Issuer Script Commands.

The principle objective of secure messaging is to ensure data confidentiality, message integrity, and issuer authentication. Message integrity and issuer authentication are achieved using a MAC. Data confidentiality is achieved using encipherment of the confidential data, such as an offline PIN, if present in the command.

- **Message Authentication (MACing)**—Message Authentication (MACing) shall be used to authenticate the issuer as the originator of the Issuer Script Command and to ensure that the command has not been altered after being sent by the issuer.

  The MAC is generated using all elements of the command, including the command header. The MAC is generated after encipherment of any confidential data in the command. The integrity of a command, including the data component contained in the command data field, if present, is ensured using secure messaging.

- **Data Confidentiality**—Data encipherment is used to ensure the confidentiality of the plaintext data required for the command. Data encipherment occurs prior to generation of the command's MAC. The data encipherment technique used needs to be known by the issuer and the currently selected application in the card.

The generation of the MAC and Data Encipherment Session Keys is described in brief in Section 14.1 Key Management for Issuer Script Processing, and in detail in Appendix B, Secure Messaging.

14.6.4 Other Considerations

If the issuer supports cardholder-selected PINs or supports PIN change by means of the PIN CHANGE/UNBLOCK command, the issuer may need the ability to change the PVV on the magnetic stripe and therefore also in the Track 2 Equivalent Data and Track 1 Discretionary Data. If the Track 2 Equivalent Data and Track 1 Discretionary Data may be updated for this reason, the issuer needs to ensure that Record 1 of SFI 1 may be updated. If updating of Record 1 is allowed, the issuer needs to impose sufficient security to ensure that the update is performed only under the issuer's control and is authorized by the issuer such that no other entity is able to update the data. The actual security procedures are left to the discretion of the issuer. Such security procedures may involve updating the record using an UPDATE RECORD command with secure messaging.

14.6.5 Resulting Indicators

The card shall use the Issuer Script Command Counter to count each command containing secure messaging that was received after the second GENERATE AC command.

The card shall set the Issuer Script Processing Failed on Last Transaction bit to "1" in the Issuer Script Failure Indicator if one of the following error conditions occurred during card processing of a command received after the second GENERATE AC command:

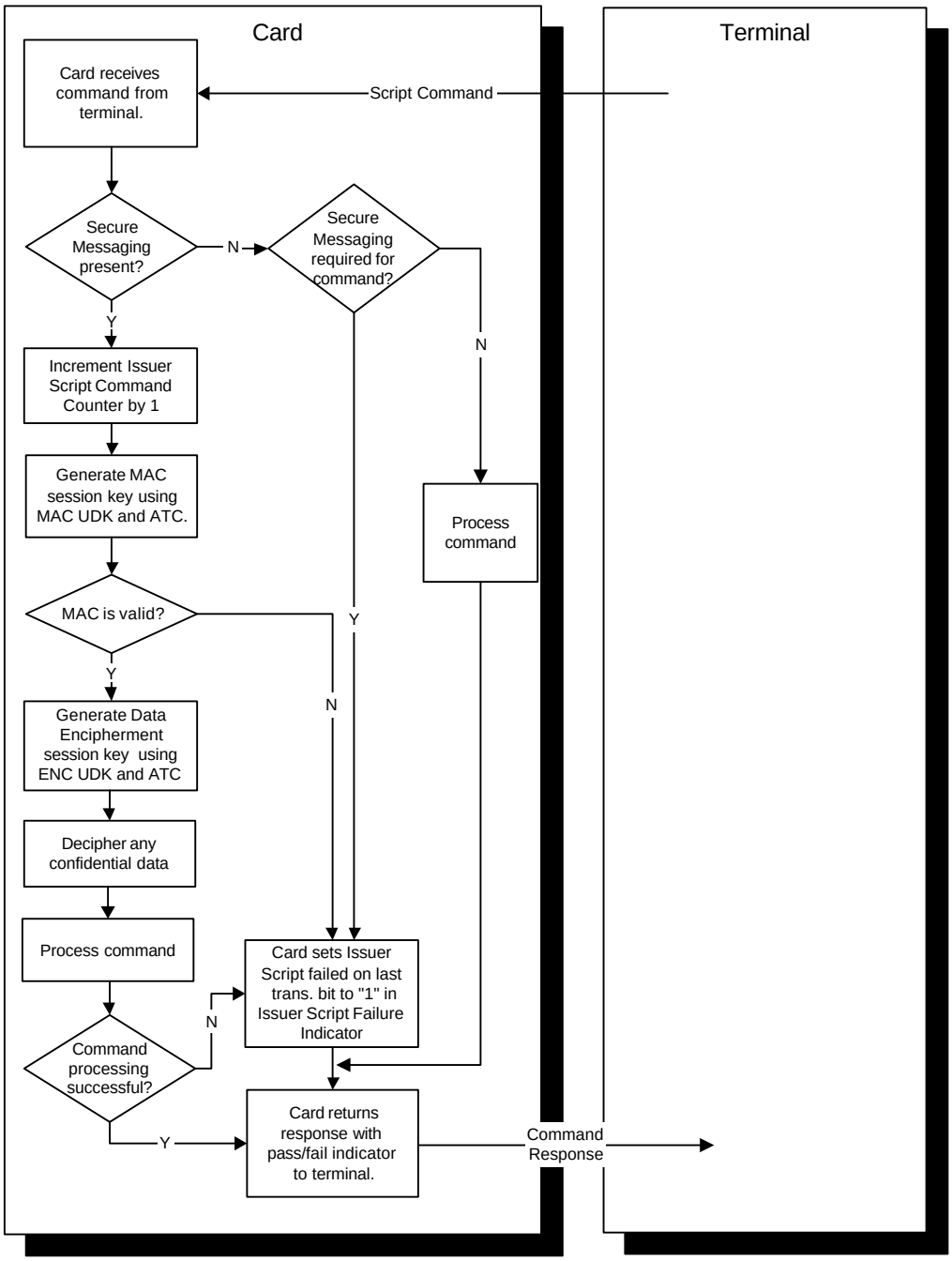
- Secure messaging is required to perform the command but was not present
- Secure messaging failed (Calculated MAC not equal to MAC in command)
- Secure messaging passed but processing of the command failed

Failure of card processing for a command that does not require secure messaging shall not impact this indicator.

14.6.6 Processing Flow

Figure 14–3 shows how a card might process each command received during Issuer-to-Card Script Processing.

Figure 14–3: Issuer-to-Card Script Processing Flow



14.7 Prior Related Processing

Online Processing

The online response received by the terminal from the acquirer may contain an Issuer Script to be processed during Issuer-to-Card Script Processing.

Completion

If the online response received from the terminal contains an Issuer Script, Issuer-to-Card Script Processing is performed after the Completion process.

14.8 Subsequent Related Processing

Card Action Analysis (subsequent transactions)

During Card Action Analysis for the card's next transaction:

- The card sets bits 8–5 in the fourth byte of the Card Verification Results (CVR) to the Issuer Script Command Counter, using the identical bit settings.
- If the Issuer Script Processing Failed on Last Transaction bit is set to "1" in the Issuer Script Failure indicator, the card sets the Issuer Script Processing Failed on Last Transaction bit to "1" in the CVR.

Completion (subsequent transactions)

The Issuer Script Failure Indicator and Issuer Script Command Counter are reset to "0" after online transactions if *any* of the following conditions exist:

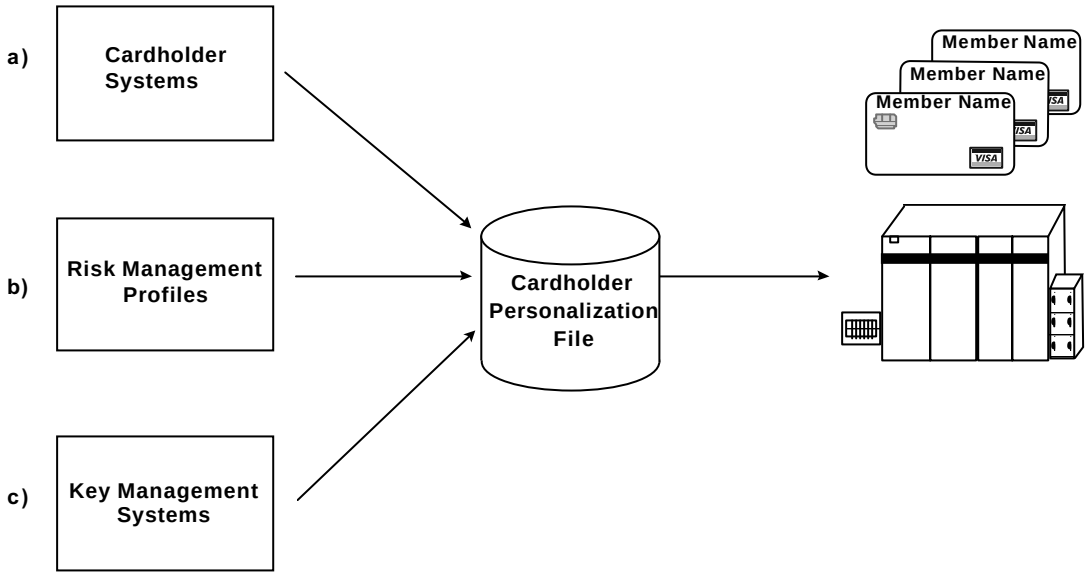
- Issuer Authentication was successful
- Issuer Authentication was optional and not performed
- Issuer Authentication was not supported

Personalization Considerations 15

Chip introduces changes to the card personalization process. Over 40 chip data elements may need to be incorporated into the card personalization process.

Information required to personalize cards is provided in Appendix F, Personalization Standards. Figure 15–1 shows a high level view of the material covered in the personalization standards.

Figure 15–1: Personalization Overview



This chapter is organized as follows:

15.1 VSDC Common Personalization

15.2 VSDC Flexible Approach

15.1 VSDC Common Personalization

Further information is provided in a separate document, *Common Personalization for Visa Smart Debit/Credit (VSDC)*, September 2000. This document is available through any of the Visa regional offices.

The intended audience for this document is designers of VSDC applications, designers of the personalization data preparation process, and Visa Smart Debit and Visa Smart Credit program managers and their technical support staff. The areas that are impacted by this document are:

- Design of the data preparation process for a VSDC application.
- Design of the file and record structure for the VSDC application on the IC card.
- Design of the IC card commands used to personalize the VSDC application
- A summary of the business decisions necessary to implement Visa Smart Debit and Visa Smart Credit risk management controls. Best-practice recommendations, where applicable, are provided for each feature.
- An overview of the data elements required on all cards as well as the additional data required for each of the optional risk control features.
- A series of technical reference implementation templates based on the best-practice recommendations for each feature and feature combinations.

15.2 VSDC Flexible Approach

In order to offer flexibility to meet the varying market needs during the migration to chip, the concept of the flexible card was developed. A flexible card is any card that offers the full functionality of the VSDC Application but allows for activation of the various features during personalization. The Application Interchange Profile (AIP) is set to "1" for each feature supported. Table 15–1 shows a card that supports SDA, Cardholder Verification, Terminal Risk Management, and Issuer Authentication.

Table 15–1: Sample Flexible Card Functionality

Byte	Bit	Value	Definition
1	8	0	Reserved for future use
1	7	1	Offline Static Data Authentication = Supported
1	6	0	Offline Dynamic Data Authentication = Not Supported
1	5	1	Cardholder Verification = Supported
1	4	1	Terminal risk management performed
1	3	1	Issuer Authentication = Supported
1	2	1	Combined DDA/AC Generation = Not Supported
1	1	0	Reserved for future use
2	8–1	0000 0000	Reserved for future use

A baseline service called Magnetic Stripe Image (MSI) is offered that only requires support of Terminal Risk Management and Cardholder Verification. MSI Cardholder Verification does not support Offline PIN.

Cryptogram Version 12 (hexadecimal "0C") is offered to support issuers that want to move to market quickly and later migrate to a more robust VSDC product. With Cryptogram Version 12, the cryptogram sent with the online authorization is not validated. The Derivation Key Index is defaulted to zero. Additional information can be found in Appendix E, Cryptogram Versions Supported, and in the *Common Personalization for Visa Smart Debit/Credit (VSDC)*, September 2000. This implementation of processing for Cryptogram Version 12 is internal to the card and is being left to individual card vendors.

Card and Issuer Data Element Tables A

This appendix defines those card data elements that may be used for financial transaction interchange and their mapping onto data objects. This includes all card and issuer data objects listed in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 3*, Annex A, and the Visa proprietary data elements. Terminal data objects from EMV are listed in the Terminal volume.

NOTE: *Although Visa does not support certain terminal-related data objects listed in the* EMV 4.0, Book 3, *Annex A, in this version of the* Visa Integrated Circuit Card Specification, *other payment systems may choose to support these data objects. Therefore, the terminal shall support all terminal-related data objects listed in those specifications.*

The data elements are presented in four tables:

- Appendix A.1 provides a description of each data element including its name, tag, format, description, and possible values.
- Appendix A.2 shows requirements for each data element.
- Appendix A.3 shows the data elements in tag sequence.
- Appendix A.4 shows indicators and counters.

A.1 Card and Issuer Data Element Descriptions

The card and issuer data elements used in Visa Smart Debit and Visa Smart Credit (VSDC) including the format (F), tag (T), and length (L) are listed in Table A–1.

The supported formats are as follows:

- n (numeric)
- cn (compressed numeric)
- b (binary)
- an (alphanumeric)
- ans (alphanumeric special)

When the length defined for the data object 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 zeros
- A data element in format cn is left-justified and padded with trailing hexadecimal Fs
- A data element in format an is left-justified and padded with trailing hexadecimal zeros
- A data element in format ans is left-justified and padded with trailing hexadecimal zeros

When data is moved from one entity to another (for example, card to terminal), it shall always be passed in order from high order to low order, regardless of how it is internally stored. The same rules apply when concatenating data.

The *Requirement* column lists the requirements for the data element:

- **M (Mandatory)**—The data element must be present and provided to the terminal. In this version of the *Visa Integrated Circuit Card* (VIS), the terminal terminates the transaction during Read Application Data if mandatory data elements are not read from the card.
- **R (Required)**—The data element must always be present. In this version of VIS, the terminal does not check for the data element during Read Application Data.
- **C (Conditional)**—The data element is necessary under the conditions specified.
- **O (Optional)**—The data element is optional.

Table A–1: Card and Issuer Data Element Descriptions (1 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Cryptogram (AC) F: b 64 T: 9F26 L: 8	R	Cryptogram returned by the ICC in the response of the GENERATE AC command (i.e., TC, ARQC, AAC, or AAR). AAR is not allowed in this version of VIS.	
Application Currency Code F: n 3 T: 9F42 L: 2	C If Cardholder Verification Method (CVM) List has amount checks	Indicates the currency in which the amount is managed according to International Organisation for Standardisation (ISO) 4217.	
Application Currency Code F: n 3 T: 9F51 L: 2	C If card velocity checking to be performed	Visa proprietary data element indicating the currency in which the account is managed according to ISO 4217.	
Application Currency Exponent F: n 1 T: 9F44 L: 1	O	Indicates the implied position of the decimal point from the right of the account represented according to ISO 4217.	

Table A–1: Card and Issuer Data Element Descriptions (2 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Default Action (ADA) F: b 16 T: 9F52 L: 2	C If Issuer Authentication supported	Visa proprietary data element indicating issuer-specified action for the card to take for certain exception conditions. This data element is required for Issuer Authentication checks. For other checks, if this data element is not present, the default value is all zeroes.	Byte 1: bit 8: 1 = If Issuer Authentication failure, transmit next transaction online bit 7: 1 = If Issuer Authentication performed and failed, decline transaction bit 6: 1 = If Issuer Authentication is mandatory and no ARPC received, decline transaction bit 5: 1 = If transaction declined offline, create advice bit 4: 1 = If PIN Try Limit exceeded on current transaction and transaction is declined, create advice bit 3: 1 = If transaction declined because issuer authentication failed or not performed, create advice bit 2: 1 = If new card, transmit transaction online bit 1: 1 = If new card, decline if unable to transmit transaction online Byte 2: bit 8: 1 = If PIN Try Limit exceeded on current transaction, block application bit 7: 1 = If PIN Try Limit exceeded on previous transaction, decline transaction bit 6: 1 = If PIN Try Limit exceeded on previous transaction, transmit transaction online bit 5: 1 = If PIN Try Limit exceeded on previous transaction, decline if unable to transmit transaction online bit 4: 1 = If issuer script failed on a previous transaction, transmit transaction online bit 3: 1 = If PIN Try Limit exceeded on previous transaction, decline and block application bits 2–1: RFU (000)

Table A–1: Card and Issuer Data Element Descriptions (3 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Discretionary Data F: b 8–256 T: 9F05 L: 1–32	O	Issuer-specified data relating to the card application.	
Application Effective Date F: n 6 YYMMDD T: 5F25 L: 3	O	Date from which the card application may be used.	
Application Expiration Date F: n 6 YYMMDD T: 5F24 L: 3	M	Date after which the card application expires.	
Application File Locator (AFL) F: var. T: 94 L: var. up to 252	R	Indicates the location (SFI, range of records) of the AEFs related to a given application.	For each file to be read, the Application File Locator contains the following 4 bytes: • Byte 1: Bits 8–4 = SFI Bits 3–1 = 000 • Byte 2: First (or only) record number to be read for that SFI (never equal to zero)· • Byte 3: Last record number to be read for that SFI (shall be greater than or equal to byte 2) • Byte 4: Number of consecutive records involved in authentication of static data, starting with record number in byte 2 (may range from zero to the value of the third byte minus the value of the second byte + 1)

Table A–1: Card and Issuer Data Element Descriptions (4 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Identifier (AID) F: b 40–128 T: 4F L: 5–16	R	Identifies the application as described in ISO/IEC 7816-5. The AID is made up of the Registered Application Provider Identifier (RID) and the Proprietary Identifier Extension (PIX)	The Visa AIDs are: A0000000031010 Visa debit or credit A0000000032010 Visa Electron A0000000033010 Interlink A0000000038010 PLUS A000000003999910 Proprietary ATM
Application Interchange Profile (AIP) F: b 16 T: 82 L: 2	M	Indicates the capabilities of the card to support specific functions in the application.	Byte 1: bit 8: 1 = Initiate (not supported) bit 7: 1 = Offline static data authentication is supported bit 6: 1 = Standard offline dynamic data authentication is supported bit 5: 1 = Cardholder verification is supported bit 4: 1 = Terminal Risk Management is to be performed bit 3: 1 = Issuer Authentication is supported bit 2: 1 = Combined DDA/AC Generation is supported bit 1: RFU (0) Byte 2: RFU (“00”)

Table A–1: Card and Issuer Data Element Descriptions (5 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Label F: an 1–16 T: 50 L: 1–16	R Will become mandatory according to EMVCo migration plan	Mnemonic associated with AID according to ISO/IEC 7816-5. Used in application selection. Application Label is optional in the File Control Information (FCI) of an Application Definition File (ADF) and mandatory in an ADF directory entry.	The Application Label shall contain “Visa” if included in the acceptance mark and shall clearly identify the payment function or product as needed to differentiate among the applications stored on the card: Visa Debit/Credit — Shall contain “Visa”. For example, “Visa”, “Visa Credit”, “Visa Debit”, or “Visa Business” Electron — Shall include “Visa” and should include “Electron”. For example “Visa” or “Visa Electron” Interlink — Shall include “Interlink”. For example, “Interlink” or “Visa Interlink” Plus — Shall include “Plus”. For example, “Plus” or “Plus ATM”
Application Preferred Name F: an 1–16 T: 9F12 L: 1–16	O	Preferred mnemonic associated with the AID. Displayed by the terminal during application selection if any of the character sets designated in the Issuer Code Table Index are supported by the terminal.	
Application Primary Account Number (PAN) F: var. up to cn 19 T: 5A L: var. up to 10	M	Valid cardholder account number.	

Table A–1: Card and Issuer Data Element Descriptions (6 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Primary Account Number (PAN) Sequence Number F: n 2 T: 5F34 L: 1	O	Identifies and differentiates card applications with the same PAN.	
Application Priority Indicator F: b 8 T: 87 L: 1	C If multiple payment applications on card	Indicates the priority of a given application or group of applications in a directory.	bit 8 = 1: Application shall not be selected without confirmation of cardholder 0: Application may be selected without confirmation of cardholder bits 7–5: RFU (000) bits 4–1: 0000 = No priority assigned xxxx = Order in which the application is to be listed or selected, ranging from 1 to 15, with 1 being the highest priority
Application Reference Currency F: n 3 T: 9F3B L: 2–8		1–4 currency codes used between the terminal and the ICC when the Transaction Currency Code is different from the Application Currency Code, each code is 3 digits according to ISO 4217. This data object is not used in this version of *VIS*.	

Table A–1: Card and Issuer Data Element Descriptions (7 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Reference Currency Exponent F: n 1 T: 9F43 L: 1–4		Indicates the implied position of the decimal point from the right of the amount, for each of the 1–4 Application Reference Currencies represented according to ISO 4217. This data object is not used in this version of *VIS*.	
Application Template F: b T: 61 L: var. up to 252	C If PSE present	Template containing one or more data objects relevant to an application directory entry according to ISO/IEC 7816-5.	
Application Transaction Counter (ATC) F: b 16 T: 9F36 L: 2	R	Counter of the number of transactions processed since personalization. Maintained by the application in the card.	Initial value is zero. It is incremented by 1 each time a transaction is performed.
Application Usage Control F: b 16 T: 9F07 L: 2	O	Indicates issuer-specified restrictions on the geographic usage and services allowed for the card application.	Byte 1: bit 8: 1 = Valid for domestic cash transactions bit 7: 1 = Valid for international cash transactions bit 6: 1 = Valid for domestic goods bit 5: 1 = Valid for international goods bit 4: 1 = Valid for domestic services bit 3: 1 = Valid for international services bit 2: 1 = Valid at ATMs bit 1: 1 = Valid at terminals other than ATMs Byte 2: bit 8: 1 = Domestic cashback allowed bit 7: 1 = International cashback allowed bits 6–1: RFU (000000) Visa restrictions on byte 1: Bits 4 and 6 shall both be set to the same value. Bits 3 and 5 shall both be set to the same value.

Table A–1: Card and Issuer Data Element Descriptions (8 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Application Version Number F: b 16 T: 9F08 L: 2	M	Version number assigned by the payment system for the application.	The Application Version Number is the version, release, and modification number in binary of the *VIS* supported by the card. For cards supporting VIS 1.3.2, the value is 132, coded in binary. For cards supporting VIS 1.4.0, the value is 140, coded in binary.
Authorization Code F: an 6 T: 89 L: 6	From Issuer. Not passed to card	Nonzero value generated by the issuer for an approved transaction.	
Authorization Response Code F: an 2 T: 8A L: 2	From Issuer or terminal	Indicates the disposition of the transaction.	Codes generated by the issuer are as indicated in ISO 8583:1987. The following codes are generated by the terminal for the following exception conditions: Y1 = Offline approved Z1 = Offline declined Y2 = Approved (after card-initiated referral) (not supported in this version of *VIS*) Z2 = Declined (after card-initiated referral) (not supported in this version of *VIS*) Y3 = Unable to go online (offline approved) Z3 = Unable to go online (offline declined)

Table A–1: Card and Issuer Data Element Descriptions (9 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Card Production Life Cycle (CPLC) History File Identifiers F: b 336 T: 9F7F L: 42	R	Visa proprietary data element that provides auditability for the card through the use of card life cycle data. It is composed of the following data elements concatenated together in the order shown: • IC Fabricator/IC Type • Operating System Identifier/Operating System Release Date/Operating System Release Level • IC Fabrication Date/IC Serial Number/IC Batch Identifier • IC Module Fabricator/IC Module Packaging Date • ICC Manufacturer/IC Embedding Date • IC Pre-Personalizer/IC Pre-Personalization Date/IC Pre-Personalization Equipment Identifier • IC Personalizer/IC Personalization Date/IC Personalization Equipment Identifier	See individual data element entries for definitions and formats. The CPLC data may be stored at the application or card level.
Card Risk Management Data Object List 1 (CDOL1) F: b T: 8C L: var. up to 252	M	List of data objects (tags and lengths) to be passed to the card application with the first GENERATE AC command.	

Table A–1: Card and Issuer Data Element Descriptions (10 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Card Risk Management Data Object List 2 (CDOL2) F: b T: 8D L: var. up to 252	M	List of data objects (tags and lengths) to be passed to the card application with the second GENERATE AC command.	
Card Verification Results (CVR) F: b 32 T: – L: 4	M	Visa proprietary data element indicating the exception conditions that occurred during the current and previous transaction.Transmitted to the terminal in the Issuer Application Data.	• Byte 1: Length indicator (“03”) • Byte 2: bits 8–7: 00 = AAC returned in second GENERATE AC 01 = TC returned in second GENERATE AC 10 = Second GENERATE AC not requested 11 = RFU bits 6–5 00 = AAC returned in first GENERATE AC 01 = TC returned in first GENERATE AC 10 = ARQC returned in first GENERATE 11 = AAR returned in first GENERATE AC (not supported in this version of the *VIS*) bit 4: 1 = Issuer Authentication performed and failed bit 3: 1 = Offline PIN performed bit 2: 1 = Offline PIN verification failed bit 1: 1 = Unable to go online

Table A–1: Card and Issuer Data Element Descriptions (11 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Card Verification Results (CVR) (continued)	M	Visa proprietary data element indicating the exception conditions that occurred during the current and previous transaction.Transmitted to the terminal in the Issuer Application Data.	• Byte 3: bit 8: 1 = Last online transaction not completed bit 7: 1 = PIN Try Limit exceeded bit 6: 1 = Exceeded velocity checking counters bit 5: 1 = New card bit 4: 1 = Issuer Authentication failure on last online transaction bit 3: 1 = Issuer Authentication not performed after online authorization bit 2: 1 = Application blocked by card because PIN Try Limit exceeded bit 1: 1 = Offline static data authentication failed on last transaction and transaction declined offline • Byte 4: bits 8–5: Number of Issuer Script Commands received after the second GENERATE AC command containing secure messaging processed on last transaction bit 4: 1 = Issuer Script processing failed on last transaction bit 3: 1 = Offline dynamic data authentication failed on last transaction and transaction declined offline bit 2: 1 = Offline dynamic data authentication performed bit 1: RFU (0) ***Note:*** *If only one GENERATE AC command is issued for a transaction, byte 2, bits 6–5 shall indicate that a TC or AAC is returned in the first GENERATE AC command and bits 8–7 shall indicate that a second GENERATE AC command was not requested.* During Initiate Application Processing, bytes 2–4 are reset to all zeros.

Table A–1: Card and Issuer Data Element Descriptions (12 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Cardholder Name F: ans 2–26 T: 5F20 L: 2–26	R In future will become conditional on presence in magnetic stripe	Indicates cardholder name according to ISO 7813	
Cardholder Name—Extended F: ans 27–45 T: 9F0B L: 27–45	O	Indicates the whole cardholder name when greater than 26 characters, using the same coding convention as in ISO 7813.	

Table A–1: Card and Issuer Data Element Descriptions (13 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Cardholder Verification Method (CVM) List F: b T: 8E L: var. up to 252	R	Identifies a prioritized list of methods of verification of the cardholder supported by the card application. ***Note:*** *The issuer may choose to initialize more than one CVM List for a single application (for example, one for domestic transactions and one for international).*	• Bytes 1–4: Amount (“X”) (binary) • Bytes 5–8: Amount (“Y”) (binary) • Byte 9 (CVM Code): bit 8: 0 = Only value for methods conforming to this specification bit 7: 1 = Apply succeeding CVM field if this CVM is unsuccessful 0 = Fail cardholder verification if this CVM is unsuccessful bits 6–1 (CVM Type): 000000 = Fail CVM processing 000001 = Plaintext PIN verification performed by ICC 000010 = Enciphered PIN verified online 000011 = Plaintext PIN verification performed by ICC and signature (paper) 000100 = Enciphered PIN verification performed by ICC 000101 = Enciphered PIN verification performed by ICC and signature (paper) 011110 = Signature (paper) 011111 = No CVM required 000100–011101 = RFU by joint payment systems 100000–101111 = RFU by individual payment systems 110000–111110 = RFU by issuer 111111 = RFU

Table A–1: Card and Issuer Data Element Descriptions (14 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Cardholder Verification Method (CVM) List (continued)			• Byte 10 (CVM Condition Code): 00 = Always 01 = If cash or cashback (includes quasi-cash) 02 = If not cash or cashback (includes quasi-cash) 03 = If terminal supports the CVM 04 = RFU 05 = RFU 06 = If transaction is in Application Currency Code and is under X value 07 = If transaction is in Application Currency Code and is over X value 08 = If transaction is in Application Currency Code and is under Y value 09 = If transaction is in Application Currency Code and is over Y value 0A–7F: RFU 80–FF: RFU by individual payment systems An additional 2 bytes is added following byte 10 for each additional CVM Code and corresponding CVM Condition.
Certificate Authority Public Key Index (PKI) F: b 8 T: 8F L: 1	C If SDA, DDA, or Offline Enciphered PIN supported	Identifies the Certificate Authority's public key in conjunction with the RID for use in offline static and dynamic data authentication.	Values assigned by Visa.
Consecutive Transaction Counter (International) F: b 8 T: – L: 1	C If international velocity check to be performed	Visa proprietary data element specifying the number of consecutive offline international (those transaction not in the card's designated currency) transactions that have occurred for that card application since the last time a transaction went online.	Initialized to zero. Incremented by 1 each time an international transaction is completed offline.

Table A–1: Card and Issuer Data Element Descriptions (15 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Consecutive Transaction Limit (International) F: b 8 T: 9F53 L: 1	C If international velocity check to be performed	Visa proprietary data element specifying the maximum number of the consecutive offline international (those transaction not in the card's designated currency) transactions allowed for that card application before a transaction is requested to go online.	
Consecutive Transaction Counter (International—Country) F: b 8 T: – L: 1	C If international—country velocity check to be performed	Visa proprietary data element specifying the number of consecutive offline international (those not in the country of issue) transactions that have occurred for that card application since the last time a transaction went online.	Initialized to zero. Incremented by 1 each time an international transaction is completed offline.
Consecutive Transaction Limit (International—Country) F: b 8 T: 9F72 L: 1	C If international—country velocity check performed	Visa proprietary data element specifying the maximum number of the consecutive offline international (those not in the country of issue) transactions allowed for that card application before a transaction goes online.	

Table A–1: Card and Issuer Data Element Descriptions (16 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Cryptogram Information Data F: b 8 T: 9F27 L: 1	R	Indicates the type of cryptogram (TC, ARQC, AAC, or AAR) returned by the card and the actions to be performed by the terminal. In this version of the VIS, the card shall never indicate to perform a referral.	bits 8–7: 00 = AAC 01 = TC 10 = ARQC 11 = AAR (not supported in this version of the VIS) bit 6–5: RFU (00) 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 xxx = All other values are RFU
Cryptogram Version Number F: b 8 T: – L: 1	R	Visa proprietary data element indicating the version of the TC/AAC/ARQC algorithm used by the application. Transmitted in the Issuer Application Data.	Values assigned by Visa. The only values supported in this version of the specification are “0A”, “0C”, and “0E”.
Cumulative Total Transaction Amount F: n 12 T: – L: 6	C If velocity check for amount to be performed	Visa proprietary data element specifying the cumulative total amount of offline domestic transactions in the designated currency (Application Currency Code) for the card application since the last completed online transaction.	Initialized to zero. Incremented by the Amount, Authorized each time a transaction in the designated currency is completed offline. Reset to zero after certain online transactions.
Cumulative Total Transaction Amount Limit F: n 12 T: 9F54 L: 6	C If velocity check for amount to be performed	Visa proprietary data element specifying the maximum total amount of offline domestic transactions in the designated currency (Application Currency Code) allowed for the card application before a transaction is forced to go online.	

Table A–1: Card and Issuer Data Element Descriptions (17 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Cumulative Total Transaction Amount Upper Limit F: n 12 T: 9F5C L: 6	C If velocity check for amount to be performed	Visa proprietary data element specifying the maximum total amount of offline transactions in the designated currency or designated and secondary currency allowed for the card application before a transaction is declined after an online transaction is unable to be performed.	
Cumulative Total Transaction Amount—Dual Currency F: n 12 T: – L: 6	C If dual currency velocity check to be performed	Visa proprietary data element specifying the cumulative total amount of offline domestic transactions in the designated currency (Application Currency Code) and a secondary currency (Secondary Application Currency Code) for the card application since the last time completed online transaction. This amount is in the designated currency.	Initialized to zero. Incremented by the Amount, Authorized each time a transaction in the designated currency is completed offline. Reset to zero after certain online transactions.

Table A–1: Card and Issuer Data Element Descriptions (18 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Cumulative Total Transaction Amount Limit—Dual Currency F: n 12 T: 9F75 L: 6	C If dual currency velocity check supported	Visa proprietary data element specifying the upper limit of the total amount of offline domestic transactions in the designated currency (Application Currency Code) and a secondary currency (Secondary Application Currency Code) allowed for that card application before a transaction is forced to go online. This limit is in the designated currency.	
Currency Conversion Factor F: 8n T: 9F73 L: 4	C If dual currency velocity check to be performed	A decimal value used in a conversion algorithm to convert the Secondary Application Currency Code to the card's domestic (Application Currency Code). Issuer Script may be used to modify this data element.	• Byte 1 bits 8–5 Number of positions the decimal separator shall be shifted from the right to obtain the factor. bits 4–1 The first digit of the currency conversion factor • Bytes 2–4 The remaining six digits of the currency conversion factor
Data Authentication Code F: b 16 T: 9F45 L: 2	O	An issuer-assigned value that is recovered by the terminal from the Signed Static Application Data during SDA. Stored in card as part of Signed Static Application Data	

Table A–1: Card and Issuer Data Element Descriptions (19 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Data Encipherment DEA Key A F: b 64 T: – L: 8	C If post-issuance PIN updates may be done	Visa proprietary data element containing an 8-byte DEA key used to support Issuer Script processing when enciphered data is contained in an Issuer Script Command. Data Encipherment DEA Key A is used for encipherment and Data Encipherment DEA Key B is used for decipherment.	
Data Encipherment DEA Key B F: b 64 T: – L: 8	C If post-issuance PIN updates may be done	Visa proprietary data element containing the second half of the double-length DEA key used to support Issuer Script processing when enciphered data is contained in an Issuer Script Command.	
Dedicated File (DF) Name F: b 40–128 T: 84 L: 5–16	R	Identifies the name of the DF as described in ISO/IEC 7816-4.	
Derivation Key Index (DKI) F: b 8 T: – L: 1	O	Visa proprietary data element identifying to the issuer the appropriate issuer's derivation key to derive the card's unique DEA keys for online card and issuer authentication. (The DKI is not used by the card.) Passed to the terminal in Issuer Application Data.	Value assigned by the issuer. If not present, the default value passed is zero.

Table A–1: Card and Issuer Data Element Descriptions (20 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Directory Definition File (DDF) Name F: b 40–128 T: 9D L: 5–16	C If directory selection supported	Identifies the name of the DF associated with a directory.	
Directory Discretionary Template F: var. T: 73 L: var. up to 252	O	Issuer discretionary part of the directory according to ISO/IEC 7816-5.	
Dynamic Data Authentication Data Object List (DDOL) F: b T: 9F49 L: var. up to 252	C If DDA supported	List of data objects (tags and lengths) to be passed to the ICC in the INTERNAL AUTHENTICATE command.	
Dynamic Data Authentication Failure Indicator F: b 1 T: – L: –	C If DDA supported	Visa proprietary data element that indicates whether offline dynamic data authentication failed on the last transaction when that transaction was declined offline.	bit 1: 1 = Offline dynamic data authentication failed on last transaction and transaction declined offline
File Control Information (FCI) Issuer Discretionary Data F: var. T: BF0C L: var. up to 222	O	Issuer discretionary part of the FCI.	

Table A–1: Card and Issuer Data Element Descriptions (21 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
File Control Information (FCI) Proprietary Template F: var. T: A5 L: var.	R	Identifies the data objects proprietary to the *EMV 4.0* in the FCI Template according to ISO/IEC 7816-4.	
File Control Information (FCI) Template F: var. T: 6F L: var. up to 252	R	Identifies the FCI template according to ISO/IEC 7816-4.	
Geographic Indicator F: b 8 T: 9F55 L: –1	C If geographic restrictions supported	Visa proprietary data element indicating whether the transaction is valid for domestic and international transactions.	bit 8: 1 = Valid for domestic transactions bit 7: 1 = Valid for international transactions bits 6–1: RFU (000000)
Integrated Circuit (IC) Batch Identifier F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the IC batch and to whom the ICs are shipped; assigned by IC fabricator for shipment tracking. Represents a portion of the Visa proprietary CPLC History File Identifier.	

Table A–1: Card and Issuer Data Element Descriptions (22 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit Card (ICC) Dynamic Data F: – T: – L: var.	C If DDA supported	Issuer-determined dynamic data generated by or stored in the ICC that is transmitted to the terminal in the signed Dynamic Application Data and may be captured by the terminal to "prove" that offline dynamic data authentication was performed.	
Integrated Circuit Card (ICC) Dynamic Number F: b T: 9F4C L: 2–8	C If DDA supported	Time-variant number generated by the card during DDA and included in the Signed Dynamic Data passed to the terminal. Recovered by the terminal.	
Integrated Circuit Card (ICC) Manufacturer F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the ICC manufacturer; assigned by payment system. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit Card (ICC) PIN Encipherment Private Key F: b T: L: N_{PE}	C If Offline Enciphered PIN supported and does not use ICC Public Key data.	ICC private key used to decipher the enciphered PIN. This data element may take various forms, such as a modulus and secret exponent or Chinese Remainder Theorem coefficients.	

Table A–1: Card and Issuer Data Element Descriptions (23 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit Card (ICC) PIN Encipherment Public Key Certificate F: b T: 9F2D L: N_{PE}	C If Offline Enciphered PIN supported and does not use ICC Public Key data.	Integrated Circuit Card (ICC) PIN Encipherment Public Key certified by the issuer.	
Integrated Circuit Card (ICC) PIN Encipherment Public Key Exponent F: b T: 9F2E L: 1 or 3	C If Offline Enciphered PIN supported and does not use ICC Public Key data.	Integrated Circuit Card (ICC) PIN Encipherment Public Key Exponent used for PIN encipherment.	
Integrated Circuit Card (ICC) PIN Encipherment Public Key Remainder F: b T: 9F2F L: $N_{PE} - N_I + 42$	C If required for Offline Enciphered PIN	Digits of the ICC PIN Encipherment Public Key Modulus that do not fit into the ICC PIN Encipherment Public Key Certificate.	
Integrated Circuit Card (ICC) Private Key F: b T: – L: N_{IC}	C If DDA is supported. If used for Offline Enciphered PIN	Private key part of the ICC public key pair used for offline dynamic data authentication. It is also used for Offline Enciphered PIN if the ICC PIN Encipherment key data is not present. This data element may take various forms, such as a modulus and secret exponent or Chinese Remainder Theorem coefficients.	

Table A–1: Card and Issuer Data Element Descriptions (24 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit Card (ICC) Public Key Exponent F: b T: 9F47 L: 1 or 3	C If DDA is supported. If used for Offline Enciphered PIN	ICC Public Key Exponent used for the verification of the Signed Dynamic Application Data. It is also used for Offline Enciphered PIN if the ICC PIN Encipherment key data is not present.	
Integrated Circuit Card (ICC) Public Key Certificate F: b T: 9F46 L: N_I	C If DDA is supported. If used for Offline Enciphered PIN	ICC Public Key certified by the issuer. It is also used for Offline Enciphered PIN if the ICC PIN Encipherment key data is not present.	
Integrated Circuit Card (ICC) Public Key Remainder F: b T: 9F48 L: $N_{IC} - N_I + 42$	C If required	Digits of the ICC Public Key Modulus which do not fit within the ICC Public Key Certificate.	
Integrated Circuit (IC) Embedding Date F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the date of IC embedding; assigned by ICC manufacturer. The date is in format YDDD, where each digit is represented by a nibble. Represents a portion of the Visa proprietary CPLC History File Identifier.	

Table A–1: Card and Issuer Data Element Descriptions (25 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit (IC) Fabrication Date F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the date fabricated; assigned by IC fabricator. The date is in format YDDD, where each digit is represented by a nibble. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Fabricator F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the IC fabricator; assigned by the payment system and stored in ROM area. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Module Fabricator F: b 16 T: See CPLC History File Identifiers L: 2	M	Represents a portion of the Visa proprietary CPLC History File Identifier. 4 nibbles identifying the module fabricator; assigned by the payment system.	
Integrated Circuit (IC) Module Packaging Date F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the date of packaging; assigned by module fabricator. The date is in format YDDD, where each digit is represented by a nibble. Represents a portion of the Visa proprietary CPLC History File Identifier.	

Table A–1: Card and Issuer Data Element Descriptions (26 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit (IC) Personalization Date F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the date of personalization; assigned by personalizer. The date is in format YDDD, where each digit is represented by a nibble. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Personalization Equipment Identifier F: b 32 T: See CPLC History File Identifiers L: 4	M	Proprietary Visa data element consisting of 8 nibbles identifying the equipment model and serial number of the personalization equipment; assigned by equipment manufacturer for equipment tracking. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Personalizer F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the IC personalizer, assigned by payment system. Represents a portion of the Visa proprietary CPLC History File Identifier.	

Table A–1: Card and Issuer Data Element Descriptions (27 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit (IC) Pre-Personalization Date F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the date of pre-personalization; assigned by pre-personalizer. The date is in format YDDD, where each digit is represented by a nibble. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Pre-Personalization Equipment Identifier F: b 32 T: See CPLC History File Identifiers L: 4	M	Proprietary Visa data element consisting of 8 nibbles identifying the equipment model and serial number of the pre-personalization equipment; assigned by equipment manufacturer for equipment tracking. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Pre-Personalizer F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the pre-personalizer; assigned by payment system. Represents a portion of the Visa proprietary CPLC History File Identifier.	

Table A–1: Card and Issuer Data Element Descriptions (28 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Integrated Circuit (IC) Serial Number F: b 32 T: See CPLC History File Identifiers L: 4	M	Proprietary Visa data element consisting of 8 nibbles identifying the IC serial number within a batch run of ICCs; normally assigned by the IC fabricator but can be pre-assigned. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Integrated Circuit (IC) Type F: b 16 T: See CPLC History File Identifiers L: 2	M	Proprietary Visa data element consisting of 4 nibbles identifying the IC type; assigned by the IC fabricator and stored in ROM area. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Issuer Action Code—Default F: b 40 T: 9F0D L: 5	R Will become mandatory in future	Specifies the issuer's conditions that cause a transaction to be declined when the ICC requests an online authorization, but the terminal is unable to complete the online transaction.	Bit assignments are identical to those for Terminal Verification Results (TVR).
Issuer Action Code—Denial F: b 40 T: 9F0E L: 5	R Will become mandatory in future	Specifies the issuer's conditions that cause the decline of a transaction without attempting to go online.	Bit assignments are identical to those for Terminal Verification Results (TVR).
Issuer Action Code—Online F: b 40 T: 9F0F L: 5	R Will become mandatory in future	Specifies the issuer's conditions that cause a transaction to be transmitted online.	Bit assignments are identical to those for Terminal Verification Results (TVR).

Table A–1: Card and Issuer Data Element Descriptions (29 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Issuer Application Data F: b T: 9F10 L: var. up to 32	R	Contains proprietary application data for transmission to the issuer in an online transaction. The first byte indicates the length of the Visa discretionary data. The next 1–15 bytes consist of the concatenated Visa discretionary data. In this version of the *VIS*, the field containing the Visa discretionary data consists of the following: • Length indicator (“06”) (1 byte) • Derivation Key Index (1 byte) • Cryptogram Version Number (1 byte) • Card Verification Results (CVR) (4 bytes, including the 1-byte length indicator) If issuer discretionary data is present, the Visa discretionary data is followed by one byte indicating the length of the issuer discretionary data. The next 1–15 bytes consist of the concatenated issuer discretionary data. In this version of *VIS*, issuer discretionary data may be supported only in national markets and not in international interchange.	

Table A–1: Card and Issuer Data Element Descriptions (30 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Issuer Authentication Data F: b 64–128 T: 91 L: 8–16	O Passed from Issuer through terminal	Issuer data transmitted to card for Issuer Authentication. In this version of VIS, the Issuer Authentication Data consists of the following: • ARPC (first 8 bytes) • Authorization Response Code (last 2 bytes) Optional Issuer data is not supported in this version of VIS.	
Issuer Authentication Failure Indicator F: b 1 T: – L: –	C If Issuer Authentication is supported	Visa proprietary data element indicating that one of the following issuer authentication error conditions occurred on the last transaction: • Issuer authentication was performed and failed • Issuer authentication was not performed and is mandatory	bit 1: 1 = Issuer authentication failure on last online transaction
Issuer Authentication Indicator F: b 8 T: 9F56 L: –1	C If Issuer Authentication Supported	Visa proprietary data element indicating when Issuer Authentication is supported, whether it is mandatory or optional.	bit 8: 1 = Issuer Authentication mandatory 0 = Issuer Authentication optional bits 7–1: RFU (0000000)

Table A–1: Card and Issuer Data Element Descriptions (31 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Issuer Code Table Index F: n 2 T: 9F11 L: 1	C If Application Preferred Name is present	Indicates the code table according to ISO 8859 for displaying the Application Preferred Name.	Values are: 01 = ISO 8859, Part 1 02 = ISO 8859, Part 2 03 = ISO 8859, Part 3 04 = ISO 8859, Part 4 05 = ISO 8859, Part 5 06 = ISO 8859, Part 6 07 = ISO 8859, Part 7 08 = ISO 8859, Part 8 09 = ISO 8859, Part 9 10 = ISO 8859, Part 10
Issuer Country Code F: n 3 T: 5F28 L: 2	C If Application Usage Control is present	Indicates the country of the issuer, represented according to ISO 3166.	
Issuer Country Code F: n 3 T: 9F57 L: 2	C If card velocity checks supported If geographic restrictions supported.	Visa proprietary data element indicating the country of the issuer, represented according to ISO 3166.	
Issuer Public Key Certificate F: b T: 90 L: N_{CA}	C If SDA, DDA, or Offline Enciph. PIN supported	Issuer's public key certified by a certificate authority for use in offline static and dynamic data authentication.	
Issuer Public Key Exponent F: b T: 9F32 L: 1 or 3	C If SDA, DDA, or Offline Enciph. PIN supported	Issuer public key exponent used for the verification of the Signed Static Application Data and the ICC Public Key Certificate.	
Issuer Public Key Remainder F: b T: 92 L: $N_I - N_{CA} + 36$	C If required	Portion of the Issuer Public Key Modulus which does not fit into the Issuer PK Certificate.	

Table A–1: Card and Issuer Data Element Descriptions (32 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Issuer Script Command F: b T: 86 L: var up to 261	O From issuer to terminal. Passed to card	Sent in authorization response from issuer when response contains issuer script. Contains command passed to card.	See Appendix C, Commands for Financial Transactions.
Issuer Script Command Counter F: b 4 T: – L: –	C If issuer script is supported	Visa proprietary data element that indicates the number of Issuer Script Commands containing secure messaging processed by the card on the last transaction.	bits 4–1: Number of Issuer Script Commands received after the second GENERATE AC command using secure messaging processed by the card during the transaction A value of "F" is equivalent to 15 or more Issuer Script Commands.
Issuer Script Identifier F: b 32 T: 9F18 L: 4	O From issuer to terminal. Not passed to card.	Sent in authorization response from issuer when response contains issuer script. Assigned by the issuer to uniquely identify the issuer script.	
Issuer Script Failure Indicator F: b 1 T: – L: –	C If issuer script is supported	Visa proprietary data element that indicates whether Issuer Script processing failed on the last transaction.	bit 1: Issuer Script processing failed on last transaction
Issuer Script Template 1 F: b T: 71 L: var.	Not supported.	Contains proprietary issuer data for transmission to the card before the second GENERATE AC command. This data object is not used in this version of *VIS*.	

Table A–1: Card and Issuer Data Element Descriptions (33 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Issuer Script Template 2 F: b T: 72 L: var.	C If issuer script supported	Contains proprietary issuer data for transmission to the card after the final GENERATE AC command.	
Issuer URL F: ans T: 5F50 L: var.	O	The URL provides the location of the Issuer's Library Server on the Internet.	
Issuer URL2 F: ans T: 9F5A L: var.	O	Visa-defined URL providing the location of an Issuer server on the Internet	
Language Preference F: an 2 T: 5F2D L: 2–8	O	1–4 languages stored in order of preference, each represented by 2 alphabetical characters according to ISO 639.	
Last Online Application Transaction Counter (ATC) Register F: b 16 T: 9F13 L: 2	C If card or terminal velocity checking or new card check to be performed	ATC value of the last transaction that went online.	Initial value is zero.
Lower Consecutive Offline Limit F: b 8 T: 9F14 L: 1	C If terminal velocity check to be performed	Issuer-specified preference for maximum number of consecutive offline transactions allowed for the application in a terminal with online capability.	

Table A–1: Card and Issuer Data Element Descriptions (34 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Lower Consecutive Offline Limit F: b 8 T: 9F58 L: 1	C If card velocity check to be performed	Visa proprietary data element indicating the issuer's preference for the maximum number of consecutive offline transactions allowed for the application in a terminal with online capability.	
Message Authentication Code (MAC) DEA Key A F: b 64 T: – L: 8	C If issuer script using secure messaging supported	Visa proprietary data element containing an 8-byte DEA key used to support Issuer Script processing when the Issuer Script Commands require the use of secure messaging. In the triple DES algorithm, the MAC DEA Key A is used for encipherment and the MAC DEA Key B is used for decipherment.	
Message Authentication Code (MAC) DEA Key B F: b 64 T: – L: 8	C If issuer script using secure messaging supported	Visa proprietary data element containing the second half of the double-length DEA key used to support Issuer Script processing when the Issuer Script Commands require the use of secure messaging.	
Offline Decline Requested by Card Indicator F: b 1 T: – L: –	C If card risk management check can generate a decline	A Visa proprietary internal indicator used during the transaction processing cycle to indicate that internal card processes have indicated that the transaction should be declined offline.	

Table A–1: Card and Issuer Data Element Descriptions (35 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Online Authorization Indicator F: b 1 T: – L: –	C If card supports Issuer Authentication or Issuer script processing	Visa proprietary data element indicating if the card requested an ARQC and the transaction was not completed.	bit 1: 1 = Online authorization required and online not completed on current or previous transaction
Online Requested by Card Indicator F: b 1 T: – L: –r		A Visa proprietary internal indicator used during the transaction processing cycle to indicate that internal card processes have indicated that the transaction should be processed online.	
Operating System Provider Identifier F: b 16 T: See CPLC History File Identifiers L: 2	R	Proprietary Visa data element consisting of 4 nibbles identifying the operating system provider; assigned by payment scheme during certification and stored in ROM area. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Operating System Release Date F: b 16 T: See CPLC History File Identifiers L: 2	R	Proprietary Visa data element consisting of 4 nibbles identifying date of the current operating system release; assigned by operating system provider and stored in ROM area. The date is in format YDDD, where each digit is represented by a nibble. Represents a portion of the Visa proprietary CPLC History File Identifier.	

Table A–1: Card and Issuer Data Element Descriptions (36 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Operating System Release Level F: b 16 T: See CPLC History File Identifiers L: 2	R	Proprietary Visa data element consisting of 4 nibbles identifying the operating system release level; assigned by the operating system provider and stored in ROM area. Represents a portion of the Visa proprietary CPLC History File Identifier.	
Personal Identification Number (PIN) Try Counter F: b 8 T: 9F17 L: 1	C If offline PIN is supported	Number of PIN tries remaining.	Initial value is set to the PIN Try Limit. Decremented by 1 each time an incorrect PIN is entered. Reset to the PIN Try Limit when the correct PIN is entered or when the PIN is changed or unblocked by the issuer.
Personal Identification Number (PIN) Try Limit F: b 8 T: – L: 1	C If offline PIN is supported	Visa proprietary data element containing the Issuer-specified maximum number of consecutive incorrect PIN tries allowed.	
Processing Options Data Object List (PDOL) F: b T: 9F38 L: var.	C If terminal data needed for Initiate Application Processing	List of terminal-related data objects (tags and lengths) requested by the card to be transmitted in the GET PROCESSING OPTIONS command.	
Proprietary Application Identifier Extensions (PIX) F: b T: – L: 0–11	R	Portion of the Application Identifier (AID) which Identifies the Application Provider's specific application according to ISO 7816-5.	The currently assigned Visa PIXs used for VSDC are: 1010—Visa Debit/Credit 2010—Electron 3010—Interlink 8010—PLUS 999910—Proprietary ATM

Table A–1: Card and Issuer Data Element Descriptions (37 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Reference PIN F: b T: – L: 8	C If offline PIN supported	Visa proprietary data element containing the PIN personalized in the card by the issuer.	
Registered Application Provider Identifier (RID) F: b T: – L: 5	R	Portion of the Application Identifier (AID) which identifies the Application Provider according to ISO 7816-5.	Visa's RID is A000000003.
Response Message Template Format 1 F: var. T: 80 L: var.	R	Contains the data objects (without tags and lengths) returned by the ICC in response to a command.	
Response Message Template Format 2 F: var. T: 77 L: var.	C If Combined DDA/AC Generation supported	Contains the data objects (with tags and lengths) returned by the ICC in response to a command.	
Secondary Application Currency Code F: n 3 T: 9F76 L: 2	C If dual currency velocity check supported	Indicates a secondary currency to be converted to the designated currency in which the account is managed (Application Currency Code) according to ISO 4217.	

Table A–1: Card and Issuer Data Element Descriptions (38 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Service Code F: n 3 T: 5F30 L: 2	O	Service code as defined on magnetic stripe tracks 1 and 2 according to ISO/IEC 7813.	
Short File Identifier (SFI) F: b 8 T: 88 L: 1	R	Used in the commands related to an application elementary file (AEF) to identify the file. The SFI data object is a binary field with three high-order bits set to zero.	Values are: 1–10: Governed by joint payment systems 11–20: Payment system specific 21–30: Issuer specific
Signed Dynamic Application Data F: b T: 9F4B L: N_{IC}	C If DDA is supported	Dynamic digital signature generated by the card and validated by the terminal during DDA.	
Signed Static Application Data (SAD) F: b T: 93 L: N_I	C If SDA is supported	Digital signature generated from critical card data elements and personalized on the card. The SAD is validated by the terminal during SDA.	
Static Data Authentication Failure Indicator F: b 1 T: – L: –	C If SDA is supported	Visa proprietary data element that indicates whether offline static data authentication failed on the last transaction when that transaction was declined offline.	bit 1: 1 = Offline static data authentication failed on last transaction and transaction declined offline
Static Data Authentication Tag List F: – T: 9F4A L: var.	C	Contains list of tags of primitive data objects whose value fields are to be included in the Signed Static Application Data or the ICC Public Key Certificate.	The SDA Tag List may not contain tags other than the tag for Application Interchange Profile (AIP).

Table A–1: Card and Issuer Data Element Descriptions (39 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Track 1 Discretionary Data F: ans T: 9F1F L: var.	R Will become optional in future	Discretionary data from track 1 of the magnetic stripe according to ISO/IEC 7813.	
Track 2 Discretionary Data F: cn T: 9F20 L: var.	Not Supported	Discretionary data from track 2 of the magnetic stripe according to ISO/IEC 7813.This data object is not supported in this version of the *VIS*.	
Track 2 Equivalent Data F: B T: 57 L: var. up to 19 n, var. up to 19 1 n4 n3 0 or n 5 n, var. hex.	M	Contains the data elements of the track 2 according to the ISO/IEC 7813, excluding start sentinel, end sentinel, and LRC, as follows: Primary Account Number Field Separator (“D”) Expiration Date (YYMM) Service Code PIN Verification Field Discretionary Data (defined by individual payment systems) Pad with “F” if needed to ensure whole bytes.	Track 2 Equivalent Data shall be stored in SFI 1 Record 1.
Transaction Certificate Data Object List (TDOL) F: b T: 97 L: var. up to 252	C If cryptogram version requires pre-hashing	List of data objects (tags and lengths) used by the terminal in generating the TC Hash Value. The cryptogram versions described in Appendix E do not use the TDOL.	

Table A–1: Card and Issuer Data Element Descriptions (40 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Unique DEA Key A F: b 64 T: – L: 8	M	Proprietary Visa data element containing an 8-byte DEA key used for Online Card Authentication, Online Issuer Authentication, and AC generation. In triple DES, the Unique DEA Key A is used for encipherment and the Unique DEA Key B is used for decipherment.	
Unique DEA Key B F: b 64 T: – L: 8	M	Proprietary Visa data element containing the second half of the double-length DEA key used for online card authentication, online issuer authentication, and AC generation.	
Upper Consecutive Offline Limit F: b 8 T: 9F23 L: 1	C If terminal velocity check is supported	Issuer-specified preference for the maximum number of consecutive offline transactions allowed for this card application before the card requires online processing.	
Upper Consecutive Offline Limit F: b 8 T: 9F59 L: 1	C If card velocity checking requires a decline if online not available.	Visa proprietary data element indicating the issuer's preference for the maximum number of consecutive offline transactions allowed for this card application before the card requires online processing.	

Table A–1: Card and Issuer Data Element Descriptions (41 of 41)

Name (Format; Tag; Length)	Requirement	Description	Values
Visa Discretionary Data F: b 56 T: – L: var 7 to 9	R	The part of Issuer Application Data defined by Visa to contain a length indicator, the Derivation Key Index, the Cryptogram Version Number, and the Card Verification Results. Issuer Application Data is passed to the terminal in the GENERATE AC response.	
VLP Available Funds F: n 12 T: 9F79 L: 6	C If ICC supports VLP option	A counter that is decremented by the Amount Authorized when a VLP transaction is approved.	
VLP Funds Limit F: n 12 T: 9F77 L: 6	C If ICC supports VLP option	A Visa proprietary data element, Issuer Limit for VLP available funds, is used to reset VLP Available Funds after an online approved transaction.	
VLP Issuer Authorization Code F: a T: 9F74 L: 6	C If ICC supports VLP option	A Visa proprietary data element containing a code indicating that the transaction was an approved VLP transaction.	"VLPxxx" where xxx is assigned by the issuer.
VLP Single Transaction Limit F: n 12 T: 9F78 L: 6	O	A Visa proprietary data element indicating the maximum amount allowed for single VLP transaction	

A.2 Card and Issuer Data Element Requirements

The requirements for card and issuer data elements are listed in Table A–2.

A.2.1 Tags

The *Tag* column lists the data element's tag.

A.2.2 Required Presence

The *Mand/Cond/Opt* column lists the requirements for the data element.

- **M (Mandatory)**—The data element must always be present. If the data element is not read by the terminal during Read Application Data, the terminal terminates the transaction.
- **R (Required)**—The data element must be present, but the terminal does not check for data element during Read Application Data.
- **C (Conditional)**—The data element is necessary under certain conditions with the next column showing code for the condition. A chart at the end of the table explains the codes used for conditions.
- **O (Optional)**—The data element is optional.

A.2.3 Data Integrity (Backup Required)

The *Backup Required* column describes the protection mechanisms applicable to each dynamic data element showing whether the data element must be backed up to preserve data integrity.

When an exceptional event occurs during normal transaction processing, such as sudden card withdrawal from the terminal's card reader, sudden power supply micro-failure, etc., card exception procedures shall be implemented to protect the integrity of the application and its related data.

Strict integrity shall be ensured for the application software program, its data file structure, its security management parameters, and its static data elements (in other words, those data elements that are initialized during personalization and are not allowed to be updated after card issuance). This implies the information shall not be lost nor modified in case of exceptional events.

Protection shall be ensured for the application dynamic data (in other words, those data elements that are updated dynamically by the card as well as those initialized during personalization and are allowed to be updated after card issuance).

These protection mechanisms shall be consistent when applied to dynamic data elements sharing the same memory cell. Static and dynamic data elements shall not share the same memory cells.

A.2.4 Update Capability

The *Update* column shows whether the data element may be updated and, if it can be updated, the command to be used for the update.

A.2.5 Retrieval Capability

The *Retrieve* column shows whether the data element may be retrieved by the terminal and the command to be used for the retrieval. If "(SD)" follows the retrieval command, the data element shall only be retrieved by special devices and not by terminals during financial transactions.

A.2.6 Static or Dynamic

The Card Risk Management data elements listed as "Static" shall never be changed but shall be retrievable by special devices using the GET DATA command. The "Dynamic" data elements shall never be updated via a command transmitted by the terminal and shall not be retrievable by the terminal.

A.2.7 Secret Data

Data elements listed as "Secret" shall be stored securely within the card for each application in one or more proprietary internal files. These data elements shall never be retrievable by a terminal or any outside source and shall never be updated with the exception of the Reference PIN. The Reference PIN may be updated using an issuer script command such as the PIN CHANGE/UNBLOCK command with secure messaging.

A.2.8 ADF or DDF Data

The *In ADF or DDF* column designates those data elements which shall be stored in a payment system's DDF or ADF directory or directories) retrievable by the READ RECORD command during Application Selection.

A.2.9 Data Requirements Chart

Table A–2: Data Requirements (1 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Application Cryptogram (AC)	9F26	R				GENERATE AC				
Application Currency Code	9F42	C	29		N	READ RECORD				Must match 9F51
Application Currency Code	9F51	C	1, 2, or 3		N	GET DATA (SD)	Static			Must match 9F42
Application Currency Exponent	9F44	C	1, 2, 3, or 29		N	READ RECORD				
Application Default Action (ADA)	9F52	C	19			GET DATA (SD)	Static			
Application Discretionary Data	9F05	O			N	READ RECORD				
Application Effective Date	5F25	O			N	READ RECORD				
Application Expiration Date	5F24	M			N	READ RECORD				
Application File Locator (AFL)	94	R			N	GET PROC OPT				

Table A–2: Data Requirements (2 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Application Identifier (AID)	4F	R			N	READ RECORD			ADF	
Application Interchange Profile (AIP)	82	M			N	GET PROC. OPTIONS				
Application Label	50	R *			N	READ RECORD SELECT			ADF	*M in future
Application Preferred Name	9F12	O			N	READ RECORD SELECT			ADF	
Application PAN	5A	M			N	READ RECORD				
Application PAN Sequence Number	5F34	O			N	READ RECORD				
Application Priority Indicator	87	C	20		N	READ RECORD SELECT			ADF	
Application Transaction Counter (ATC)	9F36	R		Backup	N	GET DATA[5,6]				
Application Usage Control	9F07	O			N	READ RECORD				
Application Version Number	9F08	M			N	READ RECORD				

Table A–2: Data Requirements (3 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Card Production Life Cycle (CPLC) History File Identifiers	9F7F	R *			N *	GET DATA (SD)				*No updates after pers-onalization
Card Risk Management Data Object List 1 (CDOL1)	8C	M			N	READ RECORD				
Card Risk Management Data Object List 2 (CDOL2)	8D	M			N	READ RECORD				
Card Verification Results (CVR)					N	GENERATE AC				Part of 9F10
Cardholder Name	5F20	R (see Other)			N	READ RECORD				C (Cond. 9) in future
Cardholder Name—Extended	9F0B	O			N	READ RECORD				
Cardholder Verification Method (CVM) List	8E	R			N	READ RECORD				
Certificate Authority Public Key Index (PKI)	8F	C	13, 30, or 31		N	READ RECORD				

Table A–2: Data Requirements (4 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Consecutive Transaction Counter (International)		C	1	Backup or default to 9F53	N	N	Dynamic			
Consecutive Transaction Limit (International)	9F53	C	1		PUT DATA	GET DATA (SD)				
Consecutive Transaction Counter (International—Country)		C	7	Backup or default to 9F72	N	N	Dynamic			
Consecutive Transaction Limit (International—Country)	9F72	C	7		PUT DATA	GET DATA (SD)				
Cryptogram Information Data	9F27	R				GENERATE AC				
Cryptogram Version Number		R			N	GENERATE AC				Part of 9F10
Cumulative Total Transaction Amount		C	2	Backup or default to 9F54	N	N	Dynamic			
Cumulative Total Transaction Amount Limit	9F54	C	2		PUT DATA	GET DATA (SD)				

Table A–2: Data Requirements (5 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Cumulative Total Transaction Amount Upper Limit	9F5C	O	2 or 3		PUT DATA	GET DATA (SD)				
Cumulative Total Transaction Amount—Dual Currency		C3	Backup or default to 9F75	N	N	N	Dynamic			
Cumulative Total Transaction Amount Limit—Dual Currency	9F75	C	3		PUT DATA	GET DATA (SD)				
Currency Conversion Factor	9F73	C	3		PUT DATA	GET DATA (SD)				
Data Authentication Code	9F45	O				READ RECORD				Part of 93
Data Encipherment DEA Keys		C	10		N	N		Secret		
Dedicated File (DF) Name	84	R			N	SELECT				
Derivation Key Index		O			N	N				Part of 9F10
Directory Definition File (DDF) Name	5D	C	11		N	READ RECORD			DDF	
Directory Discretionary Template	73	O			N	READ RECORD			ADF DDF	

Table A–2: Data Requirements (6 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Dynamic Data Authentication Data Object List (DDOL)	9F19	C	31		N	READ RECORD				
Dynamic Data Authentication Failure Indicator		C	31	Backup or default to 0	N	N	Dynamic			
File Control Information (FCI) Issuer Discretionary Data	BF0C	O			N	SELECT				
File Control Information (FCI) Proprietary Template	A5	R			N	SELECT				
File Control Information (FCI) Template	6F	R			N	SELECT				
Geographic Indicator	9F55	C	12		N	GET DATA (SD)	Static			
Integrated Circuit Card (ICC) Dynamic Data		C	31			INTERNAL AUTHENTICATE				
Integrated Circuit Card (ICC) Dynamic Number	9F4C	C	31			INTERNAL AUTHENTICATE				Part of 9F4B

Table A–2: Data Requirements (7 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
ICC PIN Encipherment Public/Private Key Data		C	13 and 14							
• Private Key		C	13 and 14		N	N		Secret		
• Public Key Certificate	9F2D	C	13 and 14		N	READ RECORD				
• Public Key Exponent	9F2E	C	13 and 14		N	READ RECORD				
• Public Key Remainder	9F2F	C	15		N	READ RECORD				
ICC Public/Private Key Data										
• Private Key		C	31		N	N		Secret		
• Public Key Exponent	9F47	C	31		N	READ RECORD				
• Public Key Certificate	9F46	C	31		N	READ RECORD				
• Public Key Remainder	9F48	C	15		N	READ RECORD				
Issuer Action Code—Default	9F0D	R *			N	READ RECORD				* M in future
Issuer Action Code—Denial	9F0E	R *			N	READ RECORD				*M in future
Issuer Action Code—Online	9F0F	R *			N	READ RECORD				*M in future

Table A–2: Data Requirements (8 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Issuer Application Data	9F10	R			N	GENERATE AC				
Issuer Authentication Data	91	O	19							
Issuer Authentication Failure Indicator		C	19	Backup or default to 0 or 1	N	N	Dynamic			
Issuer Authentication Indicator	9F56	C	19		N	GET DATA (SD)	Static			
Issuer Code Table Index	9F11	C	16		N	SELECT				
Issuer Country Code	5F28	C	17		N	READ RECORD				Must match 9F57
Issuer Country Code	9F57	C	7, 12		N	GET DATA (SD)	Static			Must match 5F28
Issuer Public Key Data										
• Issuer PK Certificate	90	C	13, 30, or 31		N	READ RECORD				
• Issuer PK Exponent	9F32	C	13, 30, or 31		N	READ RECORD				
• Issuer PK Remainder	92	C	15		N	READ RECORD				

Table A–2: Data Requirements (9 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Issuer Script Command Counter		C	18	Backup or default to 0	N	N	Dynamic			
Issuer Script Failure Indicator		C	18	Backup or default to 0 or 1	N	N	Dynamic			
Issuer Script Template 2	72	C	18							
Issuer URL	5F50	O				SELECT				
Issuer URL2	9F5A	O				SELECT				
Language Preference	5F2D	O				SELECT				
Last Online ATC Register	9F13	C	4, 5, 6, 8, or 24	Backup or default to 1	N	GET DATA[5, 6, or 24]				
Lower Consecutive Offline Limit	9F14	C	5, 6, 24	Backup	UPDATE RECORD	READ RECORD				
Lower Consecutive Offline Limit	9F58	C	4	Backup	PUT DATA	GET DATA (SD)				
Message Authentication Code (MAC) DEA Keys		C	18 and 28		N	N		Secret		

Table A–2: Data Requirements (10 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Online Authorization Indicator		C	18 or 19	Default to 1 or backup	N	N	Dynamic			
PIN Try Counter	9F17	C	21	Backup or default to limit	PIN CHANGE/ UNBLOCK	GET DATA [27]				
PIN Try Limit		C	21		N	N		Secret		
Processing Options Data Object List (PDOL)	9F38	C	22, 12			SELECT				
Reference PIN		C	21	Backup	PIN CHANGE/ UNBLOCK	N		Secret		
Response Message Template Format 1	80	R			N	N				
Secondary Application Currency Code	9F76	C	3		N	GET DATA (SD)	Static			
Service Code	5F30	O			N	READ RECORD				
Short File Identifier (SFI)	88				N	SELECT GET PROC OPT				

Table A–2: Data Requirements (11 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Signed Dynamic Application Data	9F4B	C	31		n/a	INTERNAL AUTHENTICATE				
Signed Static Application Data	93	C	30		N	READ RECORD				
Signed Data Authentication Failure Indicator		C	30	Backup or default to 0	N	N	Dynamic			
Static Data Authentication Tag List	9F4A	C	(30 or 31) and 32		N	READ RECORD				
Track 1 Discretionary Data	9F1F	R *			UPDATE RECORD[25]	READ RECORD				*O in future
Track 2 Equivalent Data	57	M			UPDATE RECORD[25]	READ RECORD				Must be SFI 1 Record 1
Transaction Certificate Data Object List (TDOL)	97	C	23		N	READ RECORD				
Unique DEA Keys		R			N	N		Secret		
Upper Consecutive Offline Limit	9F23	C	5, 6, 24	Backup	UPDATE RECORD	READ RECORD				

Table A–2: Data Requirements (12 of 12)

Name	Tag	Mand/ Cond/ Opt	Conditions	Backup Required	Update	Retrieve	Static/ Dynamic	Secret Data	In ADF or DDF	Other
Upper Consecutive Offline Limit	9F59	C	8	Backup	PUT DATA	GET DATA (SD)				
VLP Available Funds	9F79	C	33	Backup or default to 0		READ RECORD GEN AC				
VLP Funds Limit	9F77	C	33		PUT DATA	GET DATA (SD)				
VLP Issuer Authorization Code	9F74	C	33			READ RECORD				
VLP Single Transaction Limit	9F78	O	33		PUT DATA	GET DATA (SD)				

A.2.10 Key to Data Requirements Chart

The numbers and codes used in the *Conditions*, *Update*, and *Retrieve* columns of the Data Requirements Chart are described in Table A–3.

Table A–3: Data Requirements Chart Key (1 of 2)

Code	Description
SD	Retrieval of data element is only supported at special devices and is not performed during financial transactions.
1	If the Consecutive Offline Transaction—International velocity check is to be performed by card.
2	If Cumulative Offline Amount velocity check is to be performed by card
3	If Cumulative Offline Amount—Dual Currency velocity check is to be performed by card.
4	If Consecutive Offline Transaction lower limit velocity check is to be performed by card.
5	If Consecutive Offline Transaction lower limit velocity check is to be performed by terminal.
6	If Consecutive Offline Transaction upper limit velocity check is to be performed by terminal.
7	If Consecutive Offline Transactions—International Country velocity checking is to be performed by card.
8	If Consecutive Offline Transaction upper limit velocity check is to be performed by card.
9	If present in magnetic stripe.
10	If updates of Reference PIN or other confidential data is supported.
11	If Directory method of Application Selection is supported.
12	If geographic restrictions supported in Initiate Application Processing.
13	If Offline Enciphered PIN supported.
14	If ICC key pair not used for Offline Enciphered PIN.
15	If corresponding public key certificate is present and entire public key does not fit into certificate.
16	If Application Preferred Name is present.

Table A–3: Data Requirements Chart Key (2 of 2)

Code	Description
17	If Application Usage Control present.
18	If Issuer Scripts supported.
19	If Issuer Authentication supported.
20	If more than one payment application on card.
21	If Offline PIN supported.
22	If terminal data needed for Initiate Application Processing.
23	If Cryptogram Version requires pre-hashing.
24	If new card check to be performed.
25	If update of the PVV is supported.
26	If Cardholder Verification is supported.
27	If “Last PIN Attempt” is to display.
28	If secure messaging technique described in VIS is supported.
29	If any CVM List conditions use amounts.
30	If SDA supported.
31	If DDA supported.
32	If primitive data objects are to be signed.
33	If Visa Low-value Payment supported.

A.3 Card and Issuer Data Element Tags

A list of the tags allocated to the card and issuer data elements is shown in Table A–4.

A list of the tags allocated to the terminal data elements may be found in Appendix A of the Terminal Volume.

Table A–4: Card Data Element Tags (1 of 5)

Tag	Card Data Element
4F	Application Identifier (AID)
50	Application Label
57	Track 2 Equivalent Data
5A	Application PAN
5D	Directory Definition File (DDF) Name
5F20	Cardholder Name
5F24	Application Expiration Date
5F25	Application Effective Date
5F28	Issuer Country Code
5F2D	Language Preference
5F30	Service Code
5F34	Application PAN Sequence Number
5F50	Issuer URL
6F	File Control Information (FCI) Template
72	Issuer Script Template 2
73	Directory Discretionary Template
80	Response Message Template Format 1

Table A–4: Card Data Element Tags (2 of 5)

Tag	Card Data Element
82	Application Interchange Profile (AIP)
84	Dedicated File (DF) Name
87	Application Priority Indicator
88	Short File Identifier (SFI)
8C	Card Risk Management Data Object List 1 (CDOL1)
8D	Card Risk Management Data Object List 2 (CDOL2)
8E	Cardholder Verification Method (CVM) List
8F	Certificate Authority Public Key Index (PKI)
90	Issuer PK Certificate
91	Issuer Authentication Data
92	Issuer PK Remainder
93	Signed Static Application Data
94	Application File Locator (AFL)
97	Transaction Certificate Data Object List (TDOL)
9F05	Application Discretionary Data
9F07	Application Usage Control
9F08	Application Version Number
9F0B	Cardholder Name—Extended
9F0D	Issuer Action Code—Default
9F0E	Issuer Action Code—Denial
9F0F	Issuer Action Code—Online

Table A–4: Card Data Element Tags (3 of 5)

Tag	Card Data Element
9F10	Issuer Application Data
9F11	Issuer Code Table Index
9F12	Application Preferred Name
9F13	Last Online ATC Register
9F14	Lower Consecutive Offline Limit (Terminal Check)
9F17	PIN Try Counter
9F19	Dynamic Data Authentication Data Object List (DDOL)
9F1F	Track 1 Discretionary Data
9F23	Upper Consecutive Offline Limit (Terminal Check)
9F26	Application Cryptogram (AC)
9F27	Cryptogram Information Data
9F2D	ICC PIN Encipherment Public Key Certificate
9F2E	ICC PIN Encipherment Public Key Exponent
9F2F	ICC PIN Encipherment Public Key Remainder
9F32	Issuer PK Exponent
9F36	Application Transaction Counter (ATC)
9F38	Processing Options Data Object List (PDOL)
9F42	Application Currency Code
9F44	Application Currency Exponent
9F45	Data Authentication Code
9F46	ICC Public Key Certificate

Table A–4: Card Data Element Tags (4 of 5)

Tag	Card Data Element
9F47	ICC Public Key Exponent
9F48	ICC Public Key Remainder
9F4A	Static Data Authentication Tag List
9F4B	Signed Dynamic Application Data
9F4C	Integrated Circuit Card (ICC) Dynamic Number
9F51	Application Currency Code
9F52	Application Default Action (ADA)
9F53	Consecutive Transaction Limit (International)
9F54	Cumulative Total Transaction Amount Limit
9F55	Geographic Indicator
9F56	Issuer Authentication Indicator
9F57	Issuer Country Code
9F58	Lower Consecutive Offline Limit (Card Check)
9F59	Upper Consecutive Offline Limit (Card Check)
9F5A	Issuer URL2
9F5C	Cumulative Total Transaction Amount Upper Limit
9F72	Consecutive Transaction Limit (International—Country)
9F73	Currency Conversion Factor
9F74	VLP Issuer Authorization Code
9F75	Cumulative Total Transaction Amount Limit—Dual Currency
9F76	Secondary Application Currency Code

Table A–4: Card Data Element Tags (5 of 5)

Tag	Card Data Element
9F77	VLP Funds Limit
9F78	VLP Single Transaction Limit
9F79	VLP Available Funds
9F7F	Card Production Life Cycle (CPLC) History File Identifiers
A5	File Control Information (FCI) Proprietary Template
BF0C	File Control Information (FCI) Issuer Discretionary Data

A.4 Indicators and Counters

The setting or incrementation of card indicators and counters and when they are reset is listed in Table A–5. The last column shows whether the indicator or counter may be updated with an issuer script command.

Table A–5: Setting of Indicators and Counters (1 of 6)

Internal Card Data	Tag	Set/Incremented	Reset	Updateable by Script
Application Transaction Counter	9F36	Set to “0” during initialization. Incremented by 1 during Initiate Application Processing	Never	No
Card Verification Results (CVR)	Part of 9F10	Flags set during SDA, DDA, Cardholder Verification, Card Action Analysis, Completion, and Issuer Script Processing	Reset at beginning of each transaction	No
Consecutive Transaction Counter (International)		Incremented during Card Action Analysis • If transaction approved or declined offline and Application Currency Code is not equal to Transaction Currency Code	Reset to “0” if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.	No
Consecutive Transaction Limit (International)	9F53	During personalization	N/A	Yes
Consecutive Transaction Counter (International—Country)		Incremented during Card Action Analysis • If transaction approved or declined offline and Issuer Country Code is not equal to Terminal Country Code	Reset to “0” if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.	No
Consecutive Transaction Limit (International—Country)	9F72	During personalization	N/A	Yes

N/A = Not Applicable

Table A–5: Setting of Indicators and Counters (2 of 6)

Internal Card Data	Tag	Set/Incremented	Reset	Updateable by Script
Cumulative Total Transaction Amount		Incremented during Card Action Analysis • If transaction approved offline and Transaction Currency Code equals Application Currency Code	Reset to "0" if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.	No
Cumulative Total Transaction Amount Limit	9F54	During personalization	N/A	Yes
Cumulative Total Transaction Amount Upper Limit	9F5C	During personalization	N/A	Yes
Cumulative Transaction Amount—Dual Currency		Incremented during Card Action Analysis • If transaction approved offline and Transaction Currency Code is equal to the Application Currency Code or the Secondary Application Currency Code	Reset to "0" if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.	No
Cumulative Transaction Amount Limit—Dual Currency	9F75	During personalization	N/A	Yes
Dynamic Data Authentication Failure Indicator		Set to "1" during Offline Data Authentication • If DDA fails and the transaction is declined offline	Reset to "0" if online transaction (either approved or declined) and Issuer Authentication requirements are met.	No
Geographic Indicator	9F55	During personalization	N/A	N/A

N/A = Not Applicable

Table A–5: Setting of Indicators and Counters (3 of 6)

Internal Card Data	Tag	Set/Incremented	Reset	Updateable by Script
Issuer Authentication Failure Indicator		Set to “1” during Issuer Authentication Processing • If Issuer Authentication fails Set to “1” during Completion • If Issuer Authentication is mandatory and not performed	Reset to “0” when Issuer Authentication passes on a subsequent transaction.	No
Issuer Script Command Counter		Incremented by 1 during Issuer Script Processing • for each script command with secure messaging received after the last GENERATE AC command	Reset to “0” if online transaction (either approved or declined) and Issuer Authentication requirements are met.	No
Issuer Script Failure Indicator		Set to “1” during Issuer Script Processing • If Issuer Script command processing fails • If secure messaging for a command fails • If secure messaging is required and not present in command	Reset to “0” if online transaction (either approved or declined) and Issuer Authentication requirements are met.	No
Last Online ATC Register	9F13	N/A	Reset to current value of ATC if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.	No
Lower Consecutive Offline Limit	9F58	During personalization	N/A	Yes

N/A = Not Applicable

Table A–5: Setting of Indicators and Counters (4 of 6)

Internal Card Data	Tag	Set/Incremented	Reset	Updateable by Script
Offline Decline Requested by Card Indicator		Set during Card Action Analysis • If Offline PIN Verification not performed and PIN tries exceeded on previous transaction and ADA indicates decline for this condition Set during Completion • If new card and ADA indicates decline if unable to go online for this condition • If velocity checking exceeded upper limits • If Offline PIN Verification not performed and PIN tries exceeded on previous transaction and ADA indicates decline if unable to go online for this condition • If PIN Tries exceeded on a previous transaction and ADA indicates decline and block application for this condition	End of each transaction	Offline Decline Requested by Card Indicator
Online Authorization Indicator		Set to “1” during Card Action Analysis • If ARQC requested by card	Reset to “0” if online authorization (either approval or decline) and Issuer Authentication requirements are met.	No

Table A–5: Setting of Indicators and Counters (5 of 6)

Internal Card Data	Tag	Set/Incremented	Reset	Updateable by Script
Online Requested by Card Indicator		Set during Card Action Analysis • If Online Authorization Indicator = 1 • If Issuer Authentication failed or mandatory and not performed on previous transaction and ADA indicates go online • If velocity checking exceeded • If new card and ADA indicates go online for this condition • If Offline PIN Verification not performed and PIN tries exceeded on previous transaction and ADA indicates go online for this condition • If issuer script failed on a previous transaction and ADA indicates go online for this condition	End of each transaction	Online Requested by Card Indicator
PIN Try Counter	9F17	Set to PIN Try Limit during personalization. Decremented by 1 with each unsuccessful VERIFY command	Reset to PIN Try Limit after successful VERIFY command and with successful PIN CHANGE/ UNBLOCK command	Yes
PIN Try Limit		Set during personalization	Never	No
Static Data Authentication Failure Indicator		Set to “1” during Offline Data Authentication • If SDA fails and transaction is declined offline.	Reset to “1” if online transaction (either approved or declined) and Issuer Authentication requirements are met.	No
Upper Consecutive Offline Limit	9F59	During personalization	N/A	Yes

N/A = Not Applicable

Table A–5: Setting of Indicators and Counters (6 of 6)

Internal Card Data	Tag	Set/Incremented	Reset	Updateable by Script
VLP Single Transaction Limit	9F78	During personalization	N/A	Yes
VLP Funds Limit	9F77	During personalization	N/A	Yes
VLP Available Funds	9F79	Decremented during Card Action Analysis for offline approved VLP transactions	Reset to VLP Funds Limit if online transaction, final cryptogram is a TC and Issuer Authentication requirements are met.	No

N/A = Not Applicable

Secure Messaging B

Secure messaging shall be performed as described in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 2*, Section 9. The technique for implementing secure messaging described in this section is identical to the Format 2 method described in that specification and is Visa's recommended method. Issuers may elect to use another technique for implementing secure messaging if they will not require Visa processing of Issuer Scripts.

Although secure messaging may be used with a command other than the Issuer Script Commands described in Chapter 14, Issuer-to-Card Script Processing, this section describes the use of secure messaging in the context of the processing of those Issuer Script Commands.

The principle objective of secure messaging is to ensure data confidentiality, message integrity, and issuer authentication. Message integrity and issuer authentication are achieved using a MAC. Data confidentiality is achieved using encipherment of the plaintext command data (if present).

B.1 Secure Messaging Format

The secure messaging format defined in this specification is compliant with International Organisation for Standardisation (ISO) 7816-4. Secure messaging is indicated for an Issuer Script Command when the second nibble of the CLA byte is equal to hexadecimal 4. The FCI in the card indicates that the data in the command data field for that command is expected to be conveyed enciphered and should be processed as such.

B.2 Message Integrity and Authentication (MACing)

The Message Authentication Code (MAC) is generated using all elements of the command, including the command header. The integrity of a command, including the data component contained in the command data, if present, is ensured using secure messaging.

B.2.1 MAC Placement

The MAC is the last data element in the command data field.

B.2.2 MAC Length

The length of the MAC is 4 to 8 bytes. Visa recommends a length of 4 bytes for the MAC.

The length needs to be known by the originator of the command and by the currently selected application in the card. The originator of the command is assumed to be the issuer.

B.2.3 MAC Key Generation

The MAC Session Key used during secure message processing is generated using the session key generation process described in Section B.4 Session Key Generation. The MAC Session Key generation process is seeded with the card's MAC DEA Key (MAC UDK).

B.2.4 MAC Computation

MAC generation occurs after encipherment of any confidential data in the command. The MAC is generated using triple DEA encipherment as follows.

1. An initial vector is set equal to 8 bytes of hexadecimal zeros.

   NOTE: *This step may be ignored. The initial vector of all zeros does not affect the MAC algorithm result. It remains here for the purpose of consistency with industry standards.*

2. The following data is concatenated in the order specified to create a block of data:

   – CLA, INS, P1, P2, Lc

   NOTE: *Lc indicates the length of the data included in the command data field after the inclusion of the 4–8-byte MAC. For example, when generating the MAC for the APPLICATION BLOCK command, the value of Lc input to the MAC calculation is 4–8; it is never zero.*

   – Last ATC (for Issuer Script processing, this is the ATC transmitted in the request message)

   – Last Application Cryptogram (for Issuer Script processing, this is usually the ARQC transmitted in the request message; when the application has been blocked prior to transmission of the request, the Application Cryptogram is an AAC)

   – Plaintext or enciphered data contained in the command data field (if present) (for example, if the PIN is being changed, the enciphered PIN block is transmitted in the command data field).

3. This block of data is formatted into 8-byte data blocks, labeled D_1, D_2, D_3, D_4, and so forth. The last data block may be 1 to 8 bytes in length.

4. If the last data block is 8 bytes in length, an additional 8-byte data block is concatenated to the right of the last data block as follows: hexadecimal 80 00 00 00 00 00 00 00. Proceed to step 5.

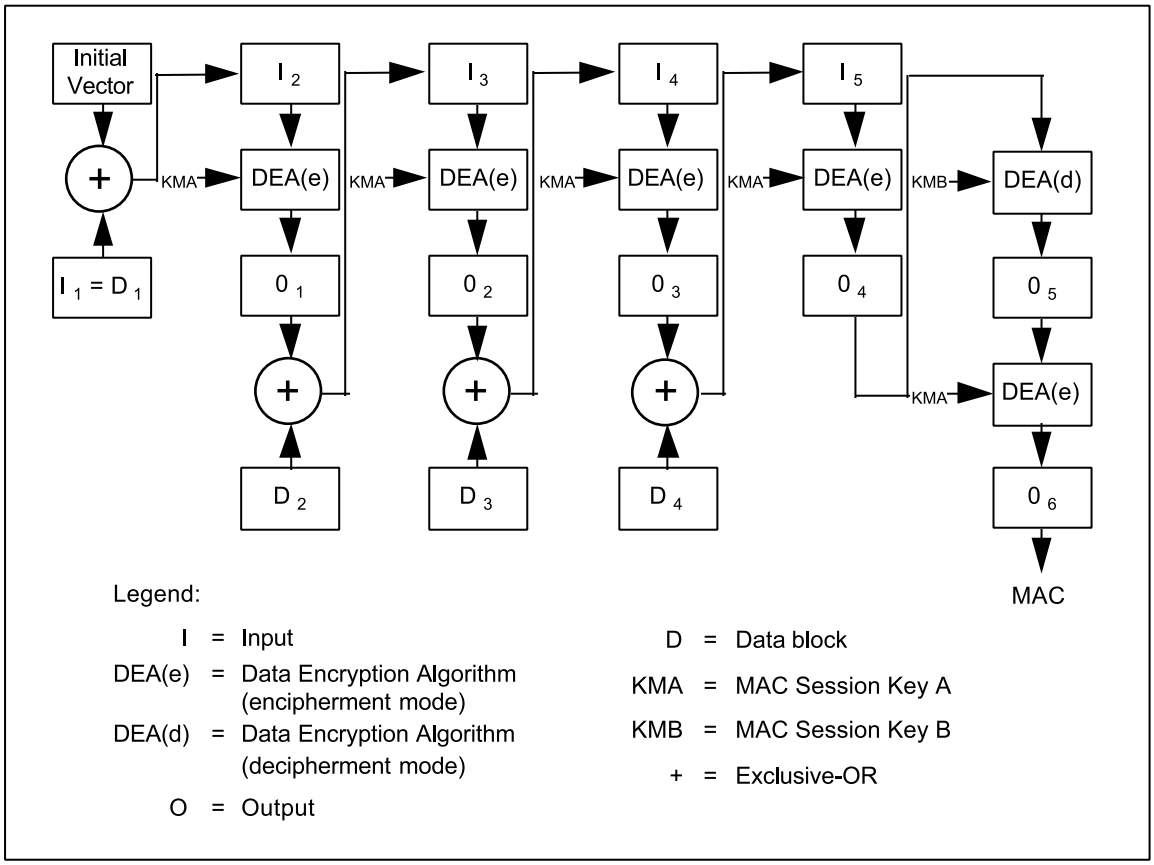
   If the last data block is less than 8 bytes in length, it is padded to the right with a 1-byte hexadecimal 80. If the last data block is now 8 bytes in length, proceed to step 5. If the last data block is still less than 8 bytes in length, it is right filled with 1-byte hexadecimal zeros until it is 8 bytes in length.

5. The data blocks are enciphered using the MAC Session Key, which is generated as described in the Section B.4 Session Key Generation.

   The MAC is generated using the MAC Session Keys A and B as shown in Figure B–1. (Depending on the length of the concatenated block of data created in step 2, there may be less than four 8-byte data blocks to input to the algorithm.)

6. The resultant value is the 8-byte MAC. If a MAC of less than eight bytes in length is desired, the right-most bytes of the MAC are truncated until the desired length is reached.

Figure B–1: MAC Algorithm for Double-Length DEA Key



B.3 Data Confidentiality

Data encipherment is used to ensure the confidentiality of the plaintext data required for the command. The data encipherment technique used needs to be known by the issuer and the currently selected application in the card.

B.3.1 Data Encipherment Key Calculation

The Data Encipherment Session Key used during secure message processing is generated as described in Chapter 14, Issuer-to-Card Script Processing, and Section B.4 Session Key Generation. The Data Encipherment Session Key generation process is seeded with the card's Data Encipherment DEA Key (ENC UDK).

B.3.2 Enciphered Data Structure

When the plaintext data required for the command is to be enciphered, it is first formatted into the following block of data:

- Length of the plaintext data, not including pad characters (L_D)
- Plaintext data
- Pad characters (as required in Section B.3.3 Data Encipherment Calculation)

The entire block of data is then enciphered using the data encipherment technique described in Section B.3.3 Data Encipherment Calculation.

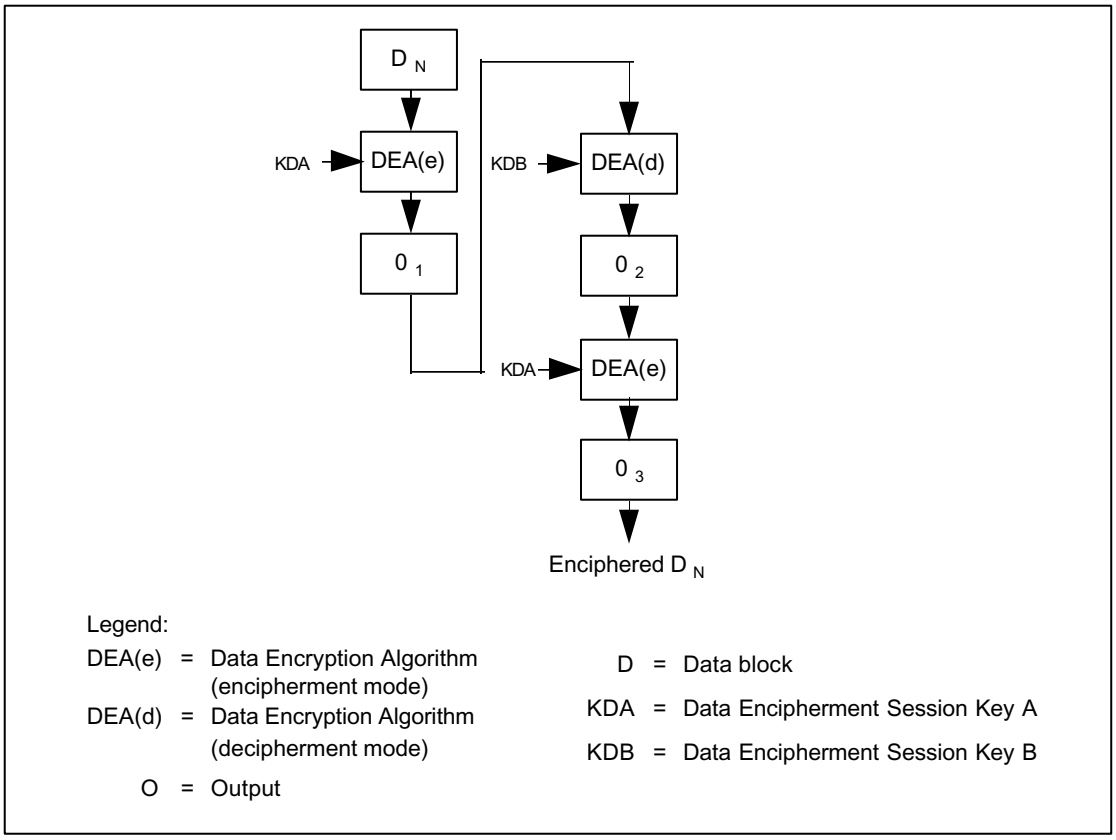
B.3.3 Data Encipherment Calculation

Data encipherment occurs prior to generation of the MAC. The data encipherment technique is as follows:

1. L_D is set equal to the length of the plaintext data. A block of data is created by prefixing L_D to the plaintext data.
2. The block of data created in step 1 is divided into 8-byte data blocks, labeled D_1, D_2, D_3, D_4, and so forth. The last data block may be 1 to 8 bytes in length.
3. If the last (or only) data block is equal to 8 bytes, proceed to step 4. If the last data block is less than 8 bytes, it is padded to the right with a hexadecimal 80. If the last data block is now equal to 8 bytes, proceed to step 4. If the last data block is still less than 8 bytes, it is right filled with 1-byte hexadecimal zeros until it is 8 bytes.
4. Each data block is enciphered using the Data Encipherment Session Key generated as described in Section B.4 Session Key Generation.

The data block is enciphered using the Data Encipherment Session Keys A and B as shown in Figure B–2.

Figure B–2: Data Encipherment for Double-Length DEA Key



5. When completed, all of the enciphered data blocks are concatenated together in order (Enciphered D_1, Enciphered D_2, and so forth). The resulting block of data is inserted in the command data field.

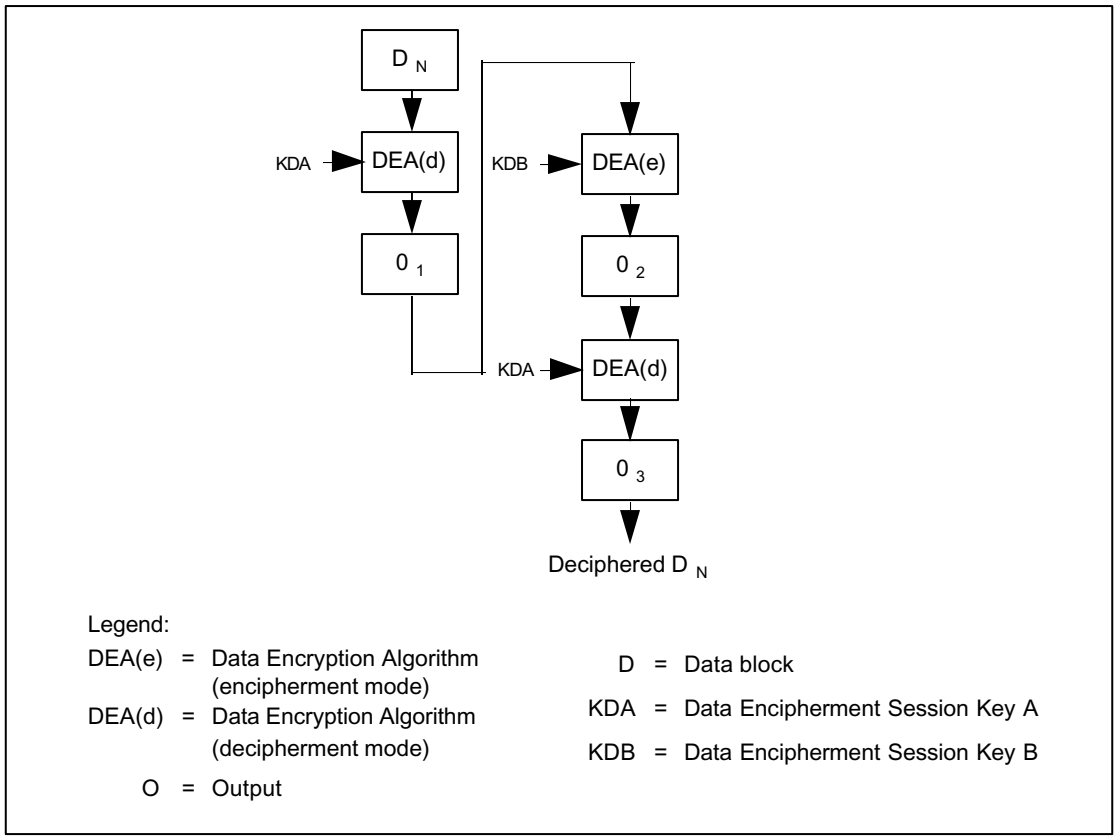
B.3.4 Data Decipherment Calculation

Upon receipt of the command, the card needs to be able to decipher the enciphered data contained in the command. The data decipherment technique is as follows:

1. The block of data contained in the command data field is divided into 8-byte blocks, labeled as D_1, D_2, D_3, D_4, and so forth. Each data block is deciphered using the Data Encipherment Session Key generated as described in Section B.4 Session Key Generation.

   The data block is deciphered using the Data Encipherment Session Keys A and B as shown in Figure B–3.

Figure B–3: Data Decipherment for Double-Length DEA Key



2. When completed, all of the deciphered data blocks are concatenated together in order (Deciphered D_1, Deciphered D_2, and so forth). The resulting block of data is composed of the recovered L_D, the recovered plaintext data, and the recovered pad characters (if added during the encipherment process described in Section B.3.3 Data Encipherment Calculation).

3. Since LD indicates the length of the plaintext data, it is used to recover the plaintext data.

B.4 Session Key Generation

This version of the *Visa Integrated Circuit Card Specification* supports either of two methods for generation of the MAC and data encipherment session keys. (The generic terms session Key A and session Key B are used within this section.) With the first method:

1. The card/issuer determines whether the MAC DEA Keys A and B (MAC UDK) or the Data Encipherment DEA Keys A and B (ENC UDK) are to be used for the selected cryptographic process.

2. The last ATC (the one transmitted in the request message) is right-justified in an 8-byte field and the remaining 6 bytes are filled with hexadecimal zeros. Session Key A is generated by performing an exclusive-OR operation on Key A with the resulting 8-byte ATC field.

3. The last ATC (the one transmitted in the request message) is inverted at the bit level by performing an exclusive-OR operation on the ATC with hexadecimal FFFF. The inverted ATC is right-justified in an 8-byte field and the remaining 6 bytes are filled with hexadecimal zeros. Session Key B is generated by performing an exclusive-OR operation on Key B with the resulting 8-byte inverted ATC field.

The second method uses the session key derivation method described in the *EMV 4.0, Book 2*, Annex A1.3.1.

B.5 Secure Messaging Impact on Command Formats

ISO/IEC 7816-4 defines four cases of command formats. This section generically describes the impact of each of these cases on the command APDU. This enables issuers that wish to use secure messaging with commands not listed in Chapter 14, Issuer-to-Card Script Processing, to implement the correct command APDU format.

NOTE: *In* EMV 4.0, *Le (the expected length of the response data field) is not shown as being present in an Issuer Script Command because only the status words are required in the response message. However,* EMV 4.0 *does not prohibit data from being transmitted in the response message.*

Case 1: This case identifies a command with no data transmitted to the ICC (Lc) and no data expected from the ICC (Le). The command format without secure messaging is as follows:

CLA	INS	P1	P2

The command format with secure messaging is as follows:

CLA	INS	P1	P2	Lc	**MAC**

The second nibble of the CLA is set to 4 to indicate support of the Format 2 secure messaging technique. Lc is set to the length of the MAC.

Case 2: This case identifies a command with no data transmitted to the ICC but data is expected from the ICC. The command format without secure messaging is as follows:

CLA	INS	P1	P2	Le

The command format with secure messaging is as follows:

CLA	INS	P1	P2	Lc	**MAC**	Le

The second nibble of the CLA is set to 4 to indicate support of the Format 2 secure messaging technique. Lc is set to the length of the MAC.

Case 3: This case identifies a command with data transmitted to the ICC but no data expected from the ICC. The command format without secure messaging is as follows:

CLA	INS	P1	P2	Lc	Command Data

The command format with secure messaging is as follows:

CLA	INS	P1	P2	Lc	Command Data	**MAC**

The second nibble of the CLA is set to 4 to indicate support of the Format 2 secure messaging technique. Lc is set to the length of the command data plus the length of the MAC.

Case 4: This case identifies a command with data transmitted to the ICC and data expected from the ICC. The command format without secure messaging is as follows:

CLA	INS	P1	P2	Lc	Command Data	Le

The command format with secure messaging is as follows:

CLA	INS	P1	P2	Lc	Command Data	**MAC**	Le

The second nibble of the CLA is set to 4 to indicate support of the Format 2 secure messaging technique. Lc is set to the length of the command data plus the length of the MAC.

Commands for Financial Transactions C

This appendix lists the commands described in the functional chapters of this document and in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 1*, Section 7, and *Book 3*, Section 2.5. These commands support transaction processing and include additional Issuer Script Commands:

- APPLICATION BLOCK (Issuer Script Command)
- APPLICATION UNBLOCK (Issuer Script Command)
- CARD BLOCK (Issuer Script Command)
- EXTERNAL AUTHENTICATE
- GENERATE APPLICATION CRYPTOGRAM
- GET CHALLENGE
- GET DATA
- GET PROCESSING OPTIONS
- INTERNAL AUTHENTICATE
- PIN CHANGE/UNBLOCK (Issuer Script Command)
- PUT DATA (Issuer Script Command)
- READ RECORD
- SELECT
- UPDATE RECORD (Issuer Script Command)
- VERIFY

These commands may be used for other purposes, such as for personalization of cards. With the exception of the GET DATA command, this section does not address requirements for the support of these commands for such purposes.

The terminal issues all commands to the card. After processing the command, the card returns a command response to the terminal. The command formats are described in the *EMV 4.0, Book 1*, Section 7, and *Book 3*, Section 2.5.

Each command includes class and instruction bytes that designate the type of command. Parameter bytes (P1 and P2) provide additional processing information. The command may include a data field.

The command response includes two status bytes (SW1 and SW2) that describe the command results. SW1 SW2 equals “9000” when the command process completes successfully. Other SW1 SW2 values are defined for specific command processing errors and warnings. The command response may include a data field.

C.1 Basic Processing Rules for Issuer Script Commands

The recommended Issuer Script commands are used to perform the functions described in Chapter 14, Issuer-to-Card Script Processing. These commands are sent by the issuer in the authorization response message and passed to the card by the terminal. Issuer Scripts for some functions such as Application Unblock and PIN Change/Unblock may be sent in non-financial transactions from special issuer-controlled devices.

Issuer Script commands require secure messaging. The recommended method of secure messaging is described in Appendix B, Secure Messaging. A Message Authentication Code (MAC) is required to validate that the command came from the valid issuer and that the command was not altered during transmission. Data encipherment is required if the command contains confidential data such as a cardholder PIN.

C.2 APPLICATION BLOCK Command—Response Application Protocol Data Units (APDUs)

The APPLICATION BLOCK command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.1.

The command data field shall contain the 4 to 8 byte MAC generated using the Format 2 method. The MAC generation process is described in Appendix B, Secure Messaging.

During personalization, multiple AIDs may be linked for blocking. This might be done when an account is represented by multiple AIDs. Blocking a single AID shall block all AIDs that were linked to that AID for blocking. One method of linking AIDs for blocking is shown in the Common Personalization for VSDC document.

C.3 APPLICATION UNBLOCK Command—Response APDUs

The APPLICATION UNBLOCK command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.2.

The command data field shall contain the 4 to 8 byte MAC generated using the Format 2 method. The MAC generation process is described in Appendix B, Secure Messaging.

During personalization, multiple AIDs may be linked for unblocking. This might be done when an account is represented by multiple AIDs. Unblocking a single AID shall unblock all AIDs that were linked to that AID for unblocking. One method of linking AIDs for unblocking is shown in the Common Personalization for VSDC document.

C.4 CARD BLOCK Command—Response APDUs

The CARD BLOCK command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.3.

The command data field shall contain the 4 to 8 byte MAC generated using the Format 2 method. The MAC generation process is described in Appendix B, Secure Messaging.

C.5 EXTERNAL AUTHENTICATE Command—Response APDUs

The EXTERNAL AUTHENTICATE command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.4. This command is used in performing online Issuer Authentication.

The card shall permit at most one EXTERNAL AUTHENTICATE command in a transaction.

The terminal transmits to the card a data object called the Issuer Authentication Data in the EXTERNAL AUTHENTICATE command. As described in the *EMV 4.0, Book 3*, Section 2.5.4, the first eight bytes contain the mandatory Authorization Response Cryptogram (ARPC), followed by an optional one to eight bytes.

In this version of the *Visa Integrated Circuit Card Specification*, the Issuer Authentication Data shall consist of the following data; optional issuer data is not supported:

- ARPC
- Authorization Response Code

The mandatory algorithm for generating and verifying the ARPC is described in Appendix D, Authentication Keys and Algorithms.

C.6 GENERATE APPLICATION CRYPTOGRAM (AC) Command—Response APDUs

The GENERATE APPLICATION CRYPTOGRAM (AC) command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.5. This command is used in generating the Authorization Request Cryptogram (ARQC), Transaction Certificate (TC), Application Authentication Cryptogram (AAC), and Application Authorization Referral (AAR). In this version of the *Visa Integrated Circuit Card Specification*, the card shall never initiate a referral so an AAR is never generated.

The mandatory algorithm for generating the TC, AAC, and ARQC is described in Appendix D, Authentication Keys and Algorithms.

Cards not capable of supporting the Combined DDA/Generate AC feature may code the data field returned in the response to the GENERATE AC command according to Format 1 as described in the *EMV 4.0, Book 3*, Section 2.5.5.4, which allows a card to transmit to the terminal a variable-length data object called the Issuer Application Data. The Issuer Application Data contains proprietary card data for online transmission.

Cards capable of supporting the Combined DDA/Generate AC feature shall code the data field returned in the GENERATE AC response according to Format 2 as described in the *EMV 4.0, Book 3*, Section 2.5.5.4. Format 2 uses BER-TLV encoding for the data elements in the response. If the response is returned in an envelope, the data returned shall be in the format shown in the *EMV 4.0, Book 2*, Table 16.

In this version of the *Visa Integrated Circuit Card Specification*, the Issuer Application Data is a mandatory data object used to transmit Visa discretionary data from the card to the terminal for input to the online request message or clearing record.

If the card receives more than two GENERATE AC commands in a transaction, the card shall response to the third and all subsequent GENERATE AC commands with an SW1 SW2 equal to “6985” and no cryptogram.

C.7 GET CHALLENGE Command—Response APDUs

The GET CHALLENGE command is optional in the card. The card shall support this command if the card supports Offline Enciphered PIN. The GET CHALLENGE command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.6.

C.8 GET DATA Command—Response APDUs

The GET DATA command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.7. Data retrievable by the GET DATA command is shown in the following section.

C.8.1 Command Support

Although this command is optional for support in the card for transaction processing, support of the GET DATA command as defined in the *EMV 4.0, Book 3*, is mandatory in the card for retrieval of the tagged Visa proprietary data listed in Table C–1 and for retrieval of the Card Production Life Cycle data listed in Appendix A, Card and Issuer Data Element Tables, during non-financial processing.

The IC operating system provider shall ensure that the GET DATA command for retrieval of Card Production Life Cycle data is capable of the following:

- Supplying the ROM and EEPROM identifiers, even if the EEPROM has not been logically structured.
- Enforcing the requirement for protection against substitution of false ROM or EEPROM data being inserted into the resulting data string.
- Protecting EEPROM data from being altered or erased, even prior to EEPROM being logically structured.
- Ensuring that the “card state” (for example, “initialized,” “pre-personalized,” or “blocked”) has no impact on the retrieval of the identifiers.

NOTE: *The operating system is not required to support the full International Organisation for Standardisation (ISO) range of the GET DATA command as described in ISO 7816-4.*

C.8.2 Data Retrievable by GET DATA Command

The following two sections show those data elements accessible at special devices using the GET DATA command with a non-financial transaction and those data elements accessible using GET DATA during a financial transaction.

C.8.2.1 Special Devices

Special devices are required to retrieve the following data for assistance in verifying the data for testing purposes:

- Card Production Life Cycle Data shall be retrievable using the tag “9F7F”. The GET DATA command shall be active at all times after IC fabrication, even prior to Application Selection. The response to the GET DATA command is a fixed-length field that consists of the entire string of identifiers concatenated together in the order specified in Appendix A, Card and Issuer Data Element Tables, beginning with the pre-defined ROM information and followed by all recorded EEPROM information. If the card has not yet been personalized with an identifier at the time that the GET DATA command is received, that identifier shall be zero filled in the response to the GET DATA command. The Card Production Life Cycle data shall be retrievable using the GET DATA command even if the card is blocked.
- The static data elements shown in Table C–1 shall be retrievable by special issuer-controlled devices using the GET DATA command if they are present on the card. Terminals shall not use the GET DATA command to retrieve this data.

Table C–1: Static Data Retrieval Using GET DATA (1 of 2)

Data Element
Application Currency Code
Application Default Action
Consecutive Transaction Limit (International Country)
Consecutive Transaction Limit (International)
Cumulative Total Transaction Amount Limit
Cumulative Total Transaction Amount Upper Limit

Table C–1: Static Data Retrieval Using GET DATA (2 of 2)

Data Element
Cumulative Total Transaction Amount Limit (Dual Currency)
Currency Conversion Factor
Geographic Indicator
Issuer Authentication Indicator
Issuer Country Code
Lower Consecutive Offline Limit
Secondary Application Currency Code
Upper Consecutive Offline Limit
VLP Funds Limit
VLP Single Transaction Limit

C.8.2.2 Financial Transactions

An issuer may choose to have the PIN Try Counter retrievable by the GET DATA command or may choose to store it as a Visa proprietary data element that cannot be accessed by a terminal.

The Visa Smart Debit/Credit application supports velocity checking by the card, not by the terminal, although terminal velocity checking is not precluded. Therefore, the Application Transaction Counter (ATC) and Last Online ATC Register are shown as stored as Visa proprietary data elements instead of as being retrievable by the GET DATA command. If an issuer elects to have terminal velocity checking performed, the card needs to support the GET DATA command to allow the terminal to retrieve the ATC and Last Online ATC Register.

If the terminal new card check is supported, retrieval of the Last Online ATC Register using GET DATA is required.

If the requested data cannot be returned because it is proprietary data, the card should return SW1 SW2 equal to “6A88” in the command response.

C.9 GET PROCESSING OPTIONS Command—Response APDUs

The GET PROCESSING OPTIONS command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.8.

Data retrievable by the GET PROCESSING OPTIONS command is shown in Table C–2.

Table C–2: Data Retrieval Using GET PROCESSING OPTIONS

Data Element
Application Interchange Profile
Application File Locator

The data field returned in the response to the GET PROCESSING OPTIONS command shall be coded according to Format 1 as described in the *EMV 4.0, Book 3*, Section 2.5.8.4.

C.10 INTERNAL AUTHENTICATE Command—Response APDUs

The INTERNAL AUTHENTICATE command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.9.

The data field returned in the response to the INTERNAL AUTHENTICATE command shall be coded according to Format 1 as described in the *EMV 4.0, Book 3*, Section 2.5.9.4.

C.11 PIN CHANGE/UNBLOCK Command—Response APDUs

The PIN CHANGE/UNBLOCK command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.10.

The command data field shall contain the PIN data (if the PIN is changing) and the four to eight byte MAC generated using the Format 2 method described in the *EMV 4.0, Book 2*, Section 9.2.1.2. The PIN data generation is described below. The encipherment of the PIN is described in Chapter 14, Issuer-to-Card Script Processing, and Appendix B, Secure Messaging. The MAC generation is described in Appendix B.

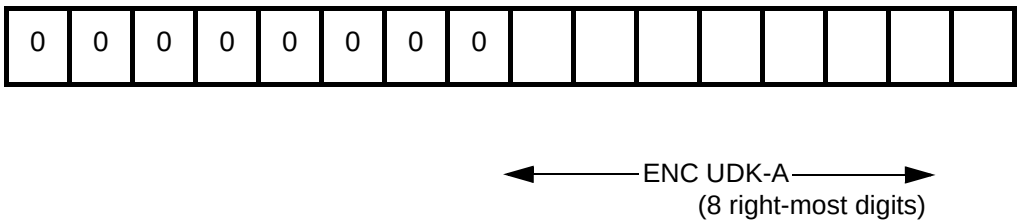
The P2 parameter indicates whether the PIN is changing and, if so, whether the current PIN is used in the generation of the PIN block. The valid P2 values are:

- **00**—PIN Unblock Only (PIN Unblock resets the PIN Try Counter to the PIN Try Limit.)
- **01**—PIN Change/Unblock with PIN data generated using current PIN (See Section C.11.1 PIN Data Generated Using the Current PIN)
- **02**—PIN Change/Unblock with PIN data generated without using current PIN (See Section C.11.2 PIN Data Generated Without Using the Current PIN)

C.11.1 PIN Data Generated Using the Current PIN

If the P2 parameter in the command is equal to 01, the PIN data is generated as follows:

1. The issuer determines the issuer's unique Data Encipherment Master Derivation Key (ENC MDK) used to generate the card application's Data Encipherment Unique DEA Key (ENC UDK).
2. The issuer determines the current Reference PIN for the card application.
3. The issuer generates the Data Encipherment Session Keys, as described in Appendix B, Secure Messaging.
4. The issuer determines the new Reference PIN for the card's application and the length of the new PIN.
5. The issuer creates a 16-hexadecimal digit PIN block as follows:
   a. Create a 16-hexadecimal digit block of data by extracting the eight right-most digits of the card application's Data Encipherment Unique DEA Key A (ENC UDK-A) and zero-filling it on the left with eight hexadecimal zeros, as shown below:



b. Create the second 16-hexadecimal digit block of data by taking the new PIN and adding a pad character of a hexadecimal zero followed by the length of the new PIN to the left of the PIN. The length N represents the number of digits (in hexadecimal) for the PIN. N is expressed as one hexadecimal digit. Right-fill the remaining bytes with hexadecimal Fs.

0	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

c. Perform an exclusive-OR operation on these two blocks of data.

6. The issuer performs an exclusive-OR operation on the PIN block created in Step 5 with the current PIN, where the current PIN is left-justified in a 16-hexadecimal digit block of data and right-filled with hexadecimal zeros. The result is called the “delta PIN.”

7. The issuer enciphers the delta PIN with the Data Encipherment Session Keys to generate the PIN data.

C.11.2 PIN Data Generated Without Using the Current PIN

If the P2 parameter in the command is equal to 02, the PIN data is generated as follows:

1. The issuer determines the issuer’s unique Data Encipherment Master Derivation Key (ENC MDK) used to generate the card application’s Data Encipherment Unique DEA Key (ENC UDK).

2. The issuer generates the Data Encipherment Session Keys, as described in Appendix B, Secure Messaging.

3. The issuer determines the new Reference PIN for the card’s application and the length of the new PIN.

4. The issuer creates a 16-hexadecimal digit PIN block as follows:

   a. Create a 16-hexadecimal digit block of data by extracting the eight right-most digits of the card application’s Data Encipherment Unique DEA Key A (ENC UDK-A) and zero-filling it on the left with eight hexadecimal zeros.

0	0	0	0	0	0	0	0								

ENC UDK-A
(8 right-most digits)

b. Create the second 16-hexadecimal digit block of data by taking the new PIN and adding a pad character of a hexadecimal zero followed by the length of the new PIN to the left of the PIN. The length N represents the number of digits (in hexadecimal) for the PIN. N is expressed as one hexadecimal digit. Right-fill with hexadecimal Fs.

0	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

c. Perform an exclusive-OR operation on these two blocks of data.

5. The issuer enciphers the PIN block created in Step 4 with the Data Encipherment Session Keys to generate the PIN data.

C.12 PUT DATA Command—Response APDUs

The PUT DATA command allows specific primitive data objects stored in the card to be updated. A data object can be updated with this command only if it has a tag associated with it. The format and use of this command is limited to updating individual primitive data objects. The use of constructed data objects is not allowed.

In this version of this specification, when the data objects in Table C–3 exist in a proprietary internal file, they may be updated using the PUT DATA command.

Table C–3: Data to be Updated With PUT DATA (1 of 2)

Data Element
Consecutive Transaction Limit (International - Country)
Consecutive Transaction Limit (International)
Cumulative Total Transaction Amount Limit
Cumulative Total Transaction Amount Limit (Dual Currency)
Cumulative Total Transaction Amount Upper Limit
Currency Conversion Factor
Lower Consecutive Offline Limit (“9F58”)

Table C–3: Data to be Updated With PUT DATA (2 of 2)

Data Element
Upper Consecutive Offline Limit (“9F59”)
VLP Funds Limit
VLP Single Transaction Limit

C.12.1 Command Message

The PUT DATA command message is coded according to Table C–4.

Table C–4: PUT DATA Command Message

Code	Value
CLA	04
INS	DA
P1 P2	Tag of data object to be updated
Lc	Length of command data field
Data	New value of data object following by MAC
Le	Not present

The command data field contains the new value of the primitive data object followed by the 4 to 8 byte MAC generated using Format 2. The MAC is generated as described in Appendix B, Secure Messaging.

C.12.2 Processing State Returned in the Response Message

A successful execution of the command is coded by 9000.

The warning conditions shown in Table C–5 may be returned by the card.

Table C–5: PUT DATA Command Message Warning Conditions

SW1	SW2	Meaning
62	00	No information given
62	81	Data may be corrupted

The error conditions shown in Table C–6 may be returned by the card.

Table C–6: PUT DATA Command Message Error Conditions

SW1	SW2	Meaning
64	00	No precise diagnosis
65	81	Memory failure
67	00	Wrong length (Lc)
68	82	Secure messaging not supported
69	82	Security status not supported
69	86	Command not allowed
69	87	Secure messaging data object missing
69	88	Secure messaging data object incorrect
6A	80	Incorrect parameter in data field
6A	81	Function not supported
6A	84	Not enough memory space in file
6A	85	Lc inconsistent with TLV structure

C.13 READ RECORD Command—Response APDUs

The READ RECORD command shall be performed as described in the *EMV 4.0, Book 1,* Section 7.2, and *Book 3*, Section 2.5.11.

C.14 SELECT Command-Response APDUs

The SELECT command shall be performed as described in the *EMV 4.0, Book 1*, Section 7.3.

As described in Part II, the following data objects shall be returned in the response to the SELECT command when the Payment System Environment (PSE) Directory is selected:

- File Control Information (FCI) Template
  - Dedicated File (DF) Name (1PAY.SYS.DDF01)
  - FCI Proprietary Template
    - Short File Identifier (SFI) of directory elementary file
    - Language Preference (optional)
    - Issuer Code Table Index (optional)
    - FCI Issuer Discretionary Data (optional)

The Issuer Code Table Index shall be present if the Application Preferred Name is present in an Application Definition File (ADF) directory entry (see Chapter 3, Application Selection)

The following data objects shall be returned when a Directory Definition File (DDF) is selected:

- FCI Template
  - DF Name
  - FCI Proprietary Template
    - SFI of directory elementary file
    - FCI Issuer Discretionary Data (optional)

The following data objects shall be returned in the response to the SELECT command when an ADF is selected, unless otherwise noted:

- FCI Template
  - DF Name
  - FCI Proprietary Template:
    - Application Label (if present in card)
    - Application Priority Indicator (if present in card)
    - Processing Options Data Object List (PDOL) (optional)
    - Language Preference (optional)
    - Issuer Code Table Index (optional)
    - Application Preferred Name (optional)
    - FCI Issuer Discretionary Data (optional)

C.15 UPDATE RECORD Command—Response APDUs

The UPDATE RECORD command is used to update a record in a file with the data provided in the command data field.

C.15.1 Command Message

The UPDATE RECORD command message is coded according to the values in Table C–7.

Table C–7: UPDATE RECORD Command Message

Code	Value
CLA	04
INS	DC
P1	Record number to be updated
P2	Reference control parameter
Lc	Length of record data and MAC
Data	Record data followed by MAC
Le	Not present

P2 is structured as shown in Table C–8.

Table C–8: UPDATE RECORD Reference Control Parameter

b8–b4	b3–b1	Meaning
Xxxxx (not all equal		SFI
	100	Record number as in P1

The command data field consists the new record followed by a four-byte to eight-byte MAC generated using Format 2. The MAC is generated as described in Appendix B, Secure Messaging.

The data for the new record is represented in whole bytes. The data in the new record is transmitted in the same format as it exists within the old record in the card.

C.15.2 Processing State Returned in the Response Message

A successful execution of the command is coded by 9000. The warning conditions shown in Table C–9 may be returned by the card.

Table C–9: UPDATE RECORD Message Warning Conditions

SW1	SW2	Meaning
62	00	No information given
62	81	Data may be corrupted

The error conditions shown in Table C–10 may be returned by the card.

Table C–10: UPDATE RECORD Message Error Conditions (1 of 2)

SW1	SW2	Meaning
64	00	No precise diagnosis
65	81	Memory failure
67	00	Wrong length (Lc)
68	82	Secure messaging not supported
69	81	Command incompatible with file organization
69	82	Security status not satisfied
69	86	Command not allowed
69	87	Secure messaging data object missing

Table C–10: UPDATE RECORD Message Error Conditions (2 of 2)

SW1	SW2	Meaning
69	88	Secure messaging data object incorrect
6A	81	Function not supported
6A	82	File not found
6A	83	Record not found
6A	84	Not enough memory space in file
6A	85	Lc inconsistent with TLV structure

C.16 VERIFY Command—Response APDUs

The VERIFY command shall be performed as described in the *EMV 4.0, Book 3*, Section 2.5.12.

This command is optional for support in the card. The card shall support the VERIFY command if the card supports offline a cardholder verification method (CVM) such as Offline PIN.

Authentication Keys and Algorithms D

This appendix describes the keys and algorithms associated with the generation of the online authentication cryptograms (Application Authentication Cryptogram (AAC), Transaction Certificate (TC), and Authorization Request Cryptogram (ARQC). Although this version of the *Visa Integrated Circuit Card Specification* does not support the generation of an Application Authorization Referral (AAR) by the card, a subsequent version may support this function.

This appendix includes the following sections:

D.1 Source Data

D.2 Generating the TC, AAC, and ARQC

D.3 Generating the Authorization Response Cryptogram (ARPC)

D.4 Data Conversion

D.5 Derivation Key Methodology

D.6 Host Security Modules (HSM)

D.1 Source Data

To support generation of a TC/AAC or ARQC, the issuer needs to decide the source for each data object input to the TC/AAC and ARQC algorithms. (In this version of the *Visa Integrated Circuit Card Specification*, the methods for generating the TC/AAC and the ARQC are identical.)

A data object to be input to the TC/AAC or ARQC algorithm is obtained by the card from one of following sources:

- It is referenced in one or both of the card's Card Data Object List (CDOLs) and is transmitted in plaintext from the terminal to the card in the GENERATE APPLICATION CRYPTOGRAM (AC) command. CDOL1 and CDOL2 are mandatory data object lists.
- To reduce the length of the data passed, data objects may be referenced in the card's Transaction Certificate Data Object List (TDOL), input by the terminal to the TC Hash Value, and passed from the terminal to the card as part of the TC Hash Value in the GENERATE AC command. The TDOL is an optional data object list. The cryptogram versions defined in Appendix E, Cryptogram Versions Supported, do not use a TDOL.
- It is accessed internally by the card. Only certain data elements (for example, Visa proprietary data elements, data objects retrievable by the GET DATA or the GET PROCESSING OPTIONS command) can be accessed internally by the card. In this version of the *Visa Integrated Circuit Card Specification*, issuer proprietary data shall not be input to the cryptograms.

Visa supports a limited set of methods to create a TC/AAC and ARQC that are each identified by a Cryptogram Version Number. Currently, Cryptogram Version Number 10 (hexadecimal 0A), 12 (hexadecimal 0C), and 14 (hexadecimal 0E) are supported. See Appendix E, Cryptogram Versions Supported, for detailed information on the Visa-supported cryptogram versions.

The Cryptogram Version Number indicates:

- The set of data used to generate the cryptogram.
- Elements from the terminal that are to be hashed before being sent to the card for generation of the cryptogram.
- The method used to generate a session key, if used.
- The method of padding the data elements prior to generating the cryptogram.

In this version of the *Visa Integrated Circuit Card Specification*, the source of the data objects is identical for both the TC/AAC and ARQC algorithms.

Table D–1 explains the TC/AAC/ARQC data element order further, including the order in which the data is processed in the following three cases:

- Data objects that are to be hashed for input to the TC Hash Value
- Data objects requested by the card in the CDOLs that are to be input to the cryptographic algorithm
- Data elements obtained internally by the card that are input to the algorithm

NOTE: *Each terminal data object is included in the cryptogram algorithm either as plaintext data or as part of the TC Hash Value data but not as both. The Visa-defined cryptogram versions do not use the TC Hash Value.*

Table D–1: TC/AAC/ARQC Data Elements Order

Data Element	Data from Terminal	Order if in TC Hash Value	Input by Card
Amount, Authorized	✓	✓	
Amount, Other	✓	✓	
Terminal Country Code	✓	✓	
Terminal Verification Results (TVR)	✓	✓	
Transaction Currency Code	✓	✓	
Transaction Date	✓	✓	
Transaction Type	✓	✓	
Unpredictable Number	✓	✓	
Application Interchange Profile (AIP)			✓
Application Transaction Counter (ATC)			✓
Card Verification Results (CVR)			✓

D.2 Generating the TC, AAC, and ARQC

The TC, AAC, and ARQC are generated by putting selected data into the algorithm described in this section. This process includes four steps:

1. In the first GENERATE AC command, the terminal shall transmit to the card the data specified in CDOL1. In the second GENERATE AC command, the terminal shall transmit to the card the data specified in CDOL2.

   If the TC Hash Value is referenced in CDOL1, the terminal shall transmit the TC Hash Value in the first and second GENERATE AC commands.

2. Based on internal card risk management, the card determines whether to return a TC/AAC or an ARQC in the response message. Because the tags and lengths for data elements not required for cryptogram generation may be contained in the CDOLs, the card shall know which data is to be input to the cryptogram algorithm. The method by which the card knows the data to be input to the cryptogram is internal to the card and is outside the scope of this specification.

   The card shall concatenate the following data in the order specified to create a block of data:

   – TC Hash Value (if present)

   – Data objects transmitted from the terminal in the GENERATE AC command for input to the cryptogram in the order specified by the cryptogram version selected. The TC Hash Value is not included.

   – Data elements input directly by the card into the cryptogram in the order specified by the cryptogram version selected.

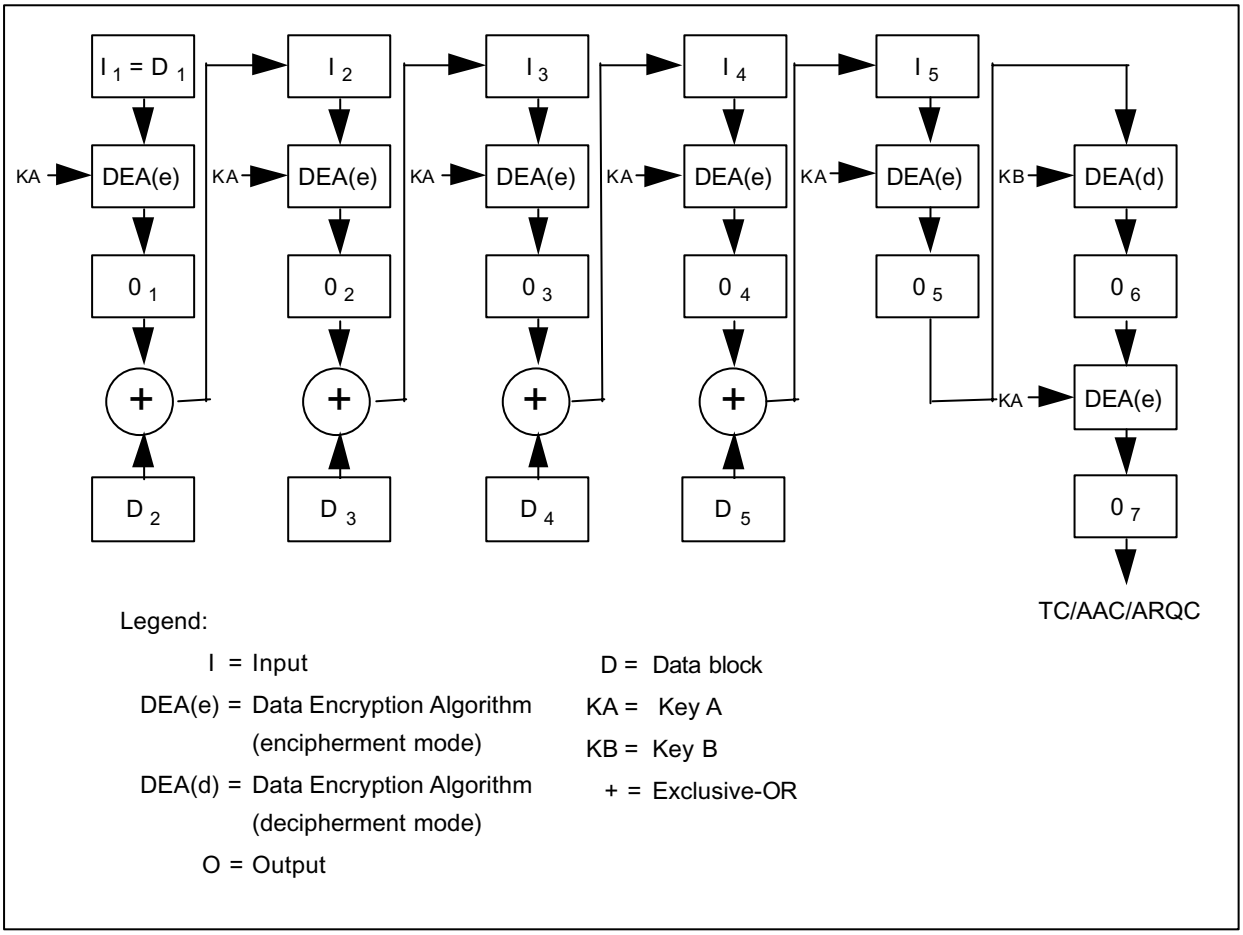
3. The card shall format this block of data into 8-byte data blocks, labeled D1, D2, D3, D4, and so on. The remaining right-most bits in the last data block shall be zero filled for Cryptogram Version 10. For Cryptogram Version 14, a mandatory “80” byte is added at the end of the significant data. The smallest number of “00’ bytes are added to right of the “80” so the last block is 8 bytes.

4. Using triple DEA encipherment, the card shall perform the algorithm shown in Figure D–1 to generate the TC/AAC or ARQC using the Unique DEA Keys A and B for Cryptogram Version 10 and the current session Keys A and B as described in Appendix E.3 Cryptogram Version 14. (Depending on the length of the concatenated data block created in Step 3, there may be fewer than five 8-byte data blocks to input to the algorithm.)

NOTE: *For Cryptogram Version 10, Key A and Key B refer to Unique DEA Key A and B. For Cryptogram Version 14, Key A and Key B refer to current session Keys A and B as described in Appendix E.3 Cryptogram Version 14.*

If Issuer Script failed, the terminal sets the "Issuer Script processing Failed after final GENERATE AC" bit in the Terminal Verification Results to "1" after the TC or AAC is generated by the card. Therefore, prior to validating the TC/AAC transmitted in the clearing message, this bit needs to be reset to "0". Otherwise, the TC/AAC cannot be correctly validated.

Figure D–1: Algorithm for Generating the TC/AAC or ARQC



D.3 Generating the Authorization Response Cryptogram (ARPC)

The Authorization Response Cryptogram (ARPC) is generated by inputting selected data into the algorithm described in this section.

The card generates a reference ARPC for comparison to the ARPC transmitted in the EXTERNAL AUTHENTICATE command. The generation process for the reference ARPC requires three steps:

1. The card shall perform an exclusive-OR operation: Application Cryptogram ⊕ Authorization Response Code.

   The Application Cryptogram used in the exclusive-OR operation shall be the cryptogram transmitted in the request message, which is usually the ARQC. Under certain processing conditions, the Application Cryptogram may be an AAC.

   The ARQC transmitted in the request message is used as input to the exclusive-OR algorithm. There is no need for the ICC to recalculate the ARQC.

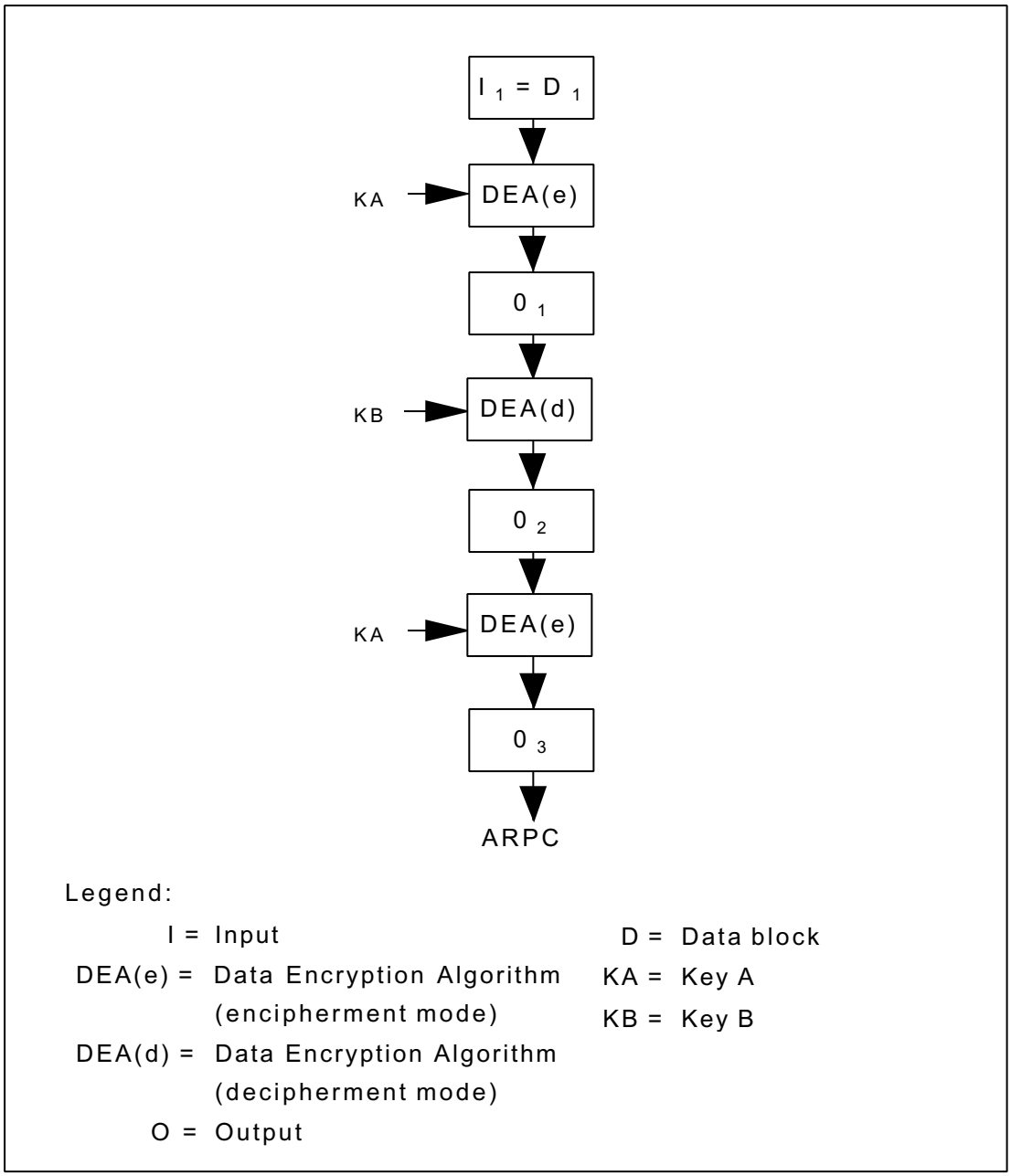
   The Authorization Response Code used in the exclusive-OR operation shall be the one transmitted to the card in the Issuer Authentication Data in the EXTERNAL AUTHENTICATE command. Prior to performing the exclusive-OR operation, the card left justifies the Authorization Response Code in an 8-byte field and zero fills (hexadecimal 0) the remaining 6 bytes (as discussed in Section D.4 Data Conversion, the Authorization Response Code is in 8-bit byte format, where each character is a 7-bit ASCII character with bit 8 always equal to zero.)

2. The results of the exclusive-OR operation shall be used as the data input to an 8-byte data block (D_1).

3. Using triple DEA encipherment, the card shall perform the authentication algorithm as shown in Figure D–2 to generate the ARPC using the Unique DEA Keys A and B for Cryptogram Version 10 and the current session Keys A and B as shown in Appendix E.3 Cryptogram Version 14. The card shall generate the ARPC by enciphering the result of the exclusive-OR operation in Step 1 with the Unique DEA Key A, deciphering that result with the Unique DEA Key B, and finally enciphering that result with the Unique DEA Key A.

   NOTE: *For Cryptogram Version 10, Key A and Key B refer to Unique DEA Key A and B. For Cryptogram Version 14, Key A and Key B refer to current session Keys A and B as described in Appendix E.3.*

Figure D–2: Algorithm for Generating the ARPC



D.4 Data Conversion

The requirements for formatting data used in the hash algorithm for generating the TC Hash Value in the cryptographic algorithms for generating the TC, AAC, ARQC, and ARPC are described in this section.

The card, terminal, and the authenticating host need to use identical data formats in the hash and cryptographic algorithms so that card and Issuer Authentication and TC validation may be performed correctly.

Since the format of the data in the card may be different than the format of the data transmitted in authorization and clearing messages, translation of data formats for input to the cryptogram algorithms may need to be performed at the issuer or at Visa.

The *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 1* and *Book 3*, define data formats for the data stored in the card and terminal that is used for the hash and cryptographic algorithms. The supported formats are:

- n (numeric)
- cn (compressed numeric)
- b (binary)
- an (alphanumeric)
- ans (alphanumeric special)

D.4.1 All Data

All data input to the hash and cryptographic algorithms by the card and terminal shall be in an 8-bit byte format.

D.4.2 Numeric Data

The card and terminal shall always input numeric data to the hash and cryptographic algorithms as two hexadecimal digits per byte (00 to 99). A numeric field with an odd number of digits shall always be padded with at least one leading hexadecimal 0.

Depending on how the numeric data is transmitted, the authenticating host may need to reformat the numeric data into the proper format for the hash and cryptographic algorithms.

D.4.3 Compressed Numeric Data

The card and terminal shall process compressed numeric data differently than numeric. A compressed numeric data element with an odd number of digits shall always be padded with at least one trailing hexadecimal F. A 3-digit compressed number stored in a 2-byte field shall be three digits (each digit is a value in the range 0–9) followed by a hexadecimal F (for example, "456F").

Depending on how the compressed numeric data is transmitted, the authenticating host may need to reformat the data into the proper format for the hash and cryptographic algorithms.

D.4.4 Binary Data

The card and terminal shall always input binary data to the hash and cryptographic algorithms as eight bits per byte. The value for any binary byte of data may vary from hexadecimal 00 to hexadecimal FF.

Depending on how the binary data is transmitted, the authenticating host may need to reformat binary data into the proper format for the hash and cryptographic algorithms.

D.4.5 Alphanumeric and Alphanumeric Special Data

Alphanumeric data transmitted in the authorization and clearing messages will normally require conversion at the authenticating host. The card and terminal shall use ASCII as the format for inputting alphanumeric data to the hash and cryptographic algorithms, where each character is a seven-bit ASCII character with bit 8 always equal to zero. The terminal shall transmit alphanumeric data to the card (for example, in the GENERATE AC command) as ASCII characters (with bit 8 equal to zero).

The authenticating host will need to convert any transmitted EBCDIC alphanumeric characters to ASCII alphanumeric characters for input to the hash and cryptographic algorithms. Alphanumeric and alphanumeric special data shall be treated identically for these algorithms.

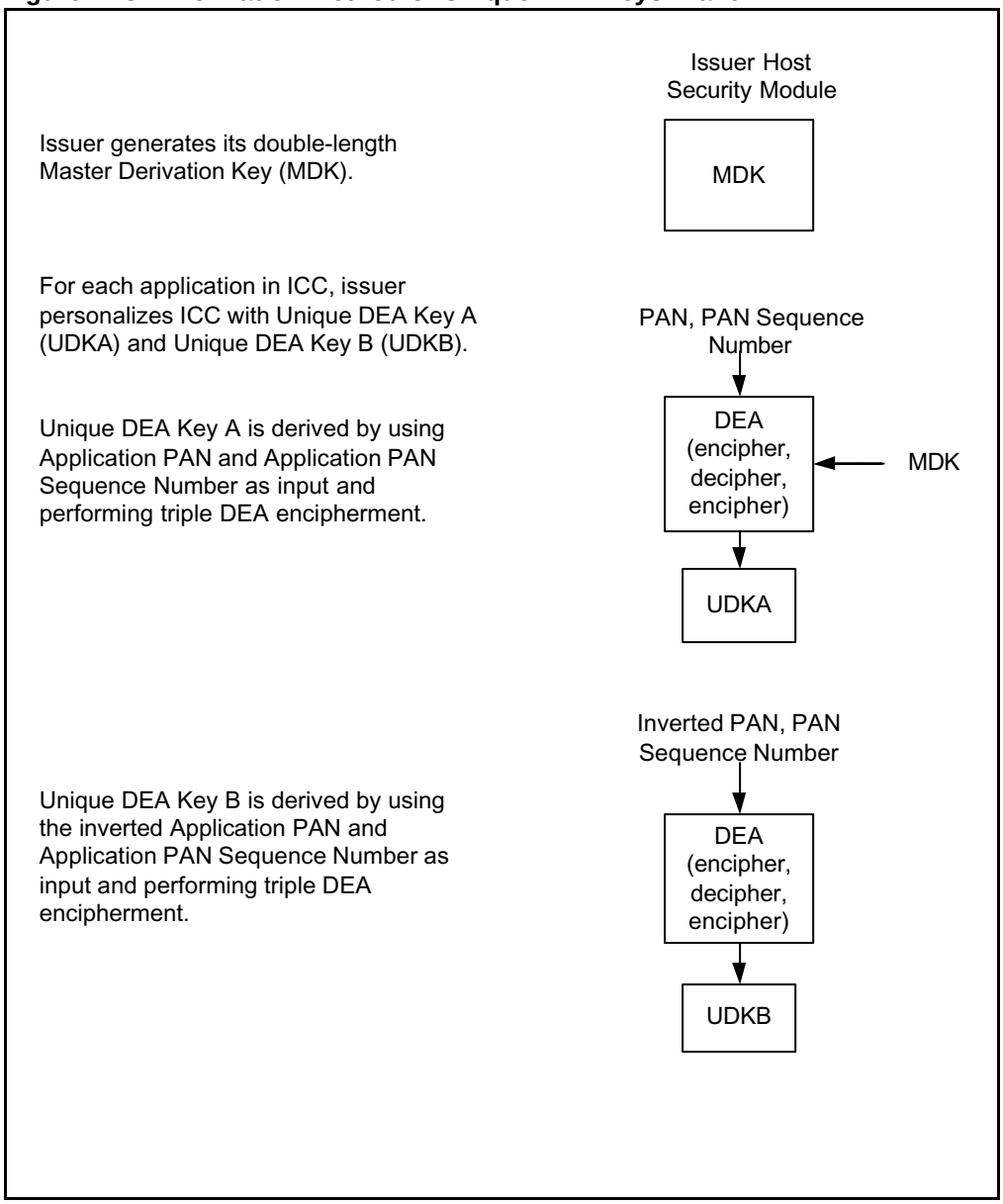
NOTE: *The Authorization Response Code shall be translated to ASCII format (with bit 8 equal to zero) prior to performing the exclusive-OR operation with the Application Cryptogram (for generating the ARPC for issuer authentication) and shall be placed in ASCII format in the Issuer Authentication Data.*

D.5 Derivation Key Methodology

This section illustrates the method of key derivation that shall be used to generate the Unique DEA Keys stored in the card during personalization. The Unique DEA Keys are used to perform online Card Authentication (generating the ARQC), online Issuer Authentication (validating the ARPC), and AAC or TC generation.

The method used for the derivation of Unique DEA Keys A and B is shown in Figure D–3.

Figure D–3: Derivation Method of Unique DEA Keys A and B



To derive the Unique DEA Key A, the Application PAN and Application PAN Sequence Number shall be concatenated together in a 16-hexadecimal field. (If the Application PAN Sequence Number is not present, it shall be zero filled.) If the length of the Application PAN followed by the Application PAN Sequence Number is not equal to 16 digits, the following formatting rules shall be applied:

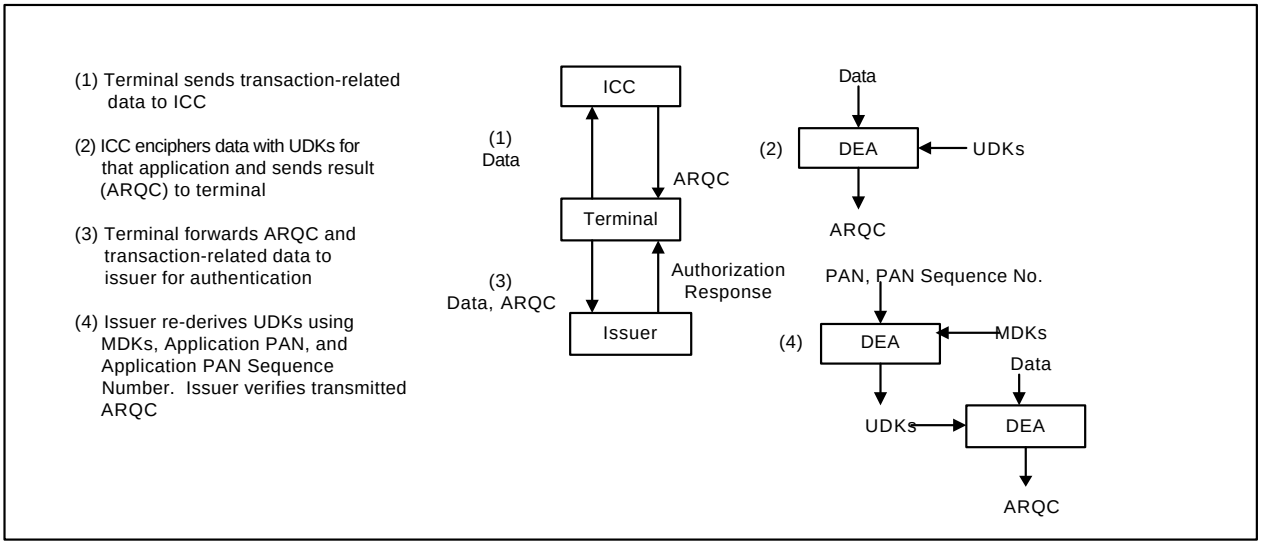
- If the Application PAN plus the Application PAN Sequence Number are less than 16 digits, right-justify the data in a 16-hexadecimal field and pad on the left with hexadecimal zeros.
- If the Application PAN followed by the Application PAN Sequence Number are greater than 16 digits, use only the right-most 16 digits.

To derive the Unique DEA Key B, the Application PAN and Application PAN Sequence Number shall first be concatenated together in a 16-hexadecimal field using the formatting rules described above and then inverted. Inversion shall be performed at the bit level, where each bit with value "1" is set to "0" and each bit with value "0" is set to "1".

NOTE: *When triple DEA encipherment is performed using the issuer's double-length Master Derivation Key, the encipherment function shall always be performed using the first half of the issuer's double-length key and the decipherment function shall always be performed using the second half of the issuer's double-length key. This convention shall apply regardless of whether the Unique DEA Key A or B is being generated.*

Figure D–4 illustrates how the Unique DEA Key A (UDKA) and Unique DEA Key B (UDKB) used by the card and the issuer to perform card authentication. A similar method is used to perform online Issuer Authentication and TC generation.

Figure D–4: Using the Unique DEA Keys to Perform Card Authentication



As shown, the derivation of the Unique DEA Keys shall be performed in a host security module and the verification of the ARQC shall also be performed in a host security module.

D.6 Host Security Modules (HSM)

A host (or hardware) security module (HSM) is a specialized International Organisation for Standardisation (ISO) 9564-1 compliant physically secure device that is used to store cryptographic functions and perform various cryptographic functions. An HSM should be used for all cryptographic functions described for the Visa Smart Debit/Credit application whenever a secret or private key is calculated or used.

Two distinct cryptographic functional areas are described below:

- Real-time host-based cryptographic functions
- Personalization support cryptographic functions

D.6.1 Real-Time Host-Based Cryptographic Functions

Real-time host-based cryptographic functions are those that are required to be performed to support processing the ARQC, TC, and AAC (which are collectively known as Application Cryptograms) and the ARPC. The specific processes to be performed within the secure confines of a hardware security module are:

- The derivation of the card's double-length Unique DEA Key using the issuer's double-length Master Derivation Key to support the verification of an Application Cryptogram and the generation of the ARPC. This process is described in Section D.5 Derivation Key Methodology.
- The verification of an Application Cryptogram and the generation of an ARPC to support a transaction. The method used by the card to generate the Application Cryptogram and the ARPC is described in Section D.2 Generating the TC, AAC, and ARQC and Section D.3 Generating the Authorization Response Cryptogram (ARPC).

D.6.2 Personalization Support Cryptographic Functions

Personalization support cryptographic functions are those functions that are required to be performed to calculate secret (or secretly derived) data to be personalized for each ICC application. The specific processes to be performed within the secure confines of a hardware security module are:

- The original derivation of the card's double-length Unique DEA Key using the issuer's double-length Master Derivation Key. This process is described in Section D.5 Derivation Key Methodology.
- The original derivation of the card's double-length MAC DEA Key using the issuer's double-length Master MAC Derivation Key. The key derivation process should be the same as that used to derive the Unique DEA Key, as described in Section D.5 Derivation Key Methodology.
- The original derivation of the card's double-length Data Encipherment DEA Key using the issuer's double-length Master Data Encipherment Key. The key derivation process should be the same as that used to derive the Unique DEA Key, as described in Section D.5 Derivation Key Methodology.
- The calculation of the Signed Static Application Data for an application using the issuer's private key part of the RSA key pair. This process is described in the *EMV 4.0, Book 2*, Section 5.
- The calculation of the ICC Public Key Certificate and ICC PIN Encipherment Public Key Certificate using the issuer's private key part of the RSA key pair. This process is described in the *EMV 4.0, Book 2*, Section 6.
- The original generation of the card's RSA key pair if offline dynamic data authentication is supported.
- The calculation and/or transference of the cardholder's PIN onto the ICC.

Cryptogram Versions Supported E

Visa supports three methods to create a Transaction Certificate (TC)/Application Authentication Cryptogram (AAC) and Authorization Request Cryptogram (ARQC). Each method is identified by a Cryptogram Version Number. Currently Cryptogram Version Number 10 (hexadecimal 0A), Cryptogram Version 12 (hexadecimal 0C), and Cryptogram Version 14 (hexadecimal 0E) are supported. The Cryptogram Version Number indicates:

- The set of data used to generate the cryptogram (Table E–1 lists the 11 mandatory data elements required for Cryptogram Version Number 10)
- Whether terminal hashing of a Visa-specified subset of that data is supported (terminal hashing is not supported for Cryptogram Version Numbers 10 or 14)
- The method used to generate a session key, if used
- The method of padding the data elements prior to generating the cryptogram.

This appendix includes the following sections:

E.1 Cryptogram Version 10

E.2 Cryptogram Version 12

E.3 Cryptogram Version 14

E.1 Cryptogram Version 10

The method for creating a TC, AAC, or ARQC using Cryptogram Version Number 10 is described in Table E–1 and illustrates:

- The order in which the data is to be input to the cryptographic algorithm
- Data objects requested by the card in the Card Data Object List (CDOL) that are to be input to the cryptographic algorithm
- Data elements obtained internally by the card that are to be input to the algorithm

Table E–1: Creating a TC/AAC and ARQC With Cryptogram Version 10

Data Element	Plaintext Data from Terminal CDOL1 and 2	Input by Card
Amount, Authorized	✓	
Amount, Other	✓	
Terminal Country Code	✓	
Terminal Verification Results (TVR)	✓	
Transaction Currency Code	✓	
Transaction Date	✓	
Transaction Type	✓	
Unpredictable Number	✓	
Application Interchange Profile		✓
ATC		✓
Card Verification Results		✓

Because the format of the data in the card may be different than the format of the data transmitted in authorization and clearing messages, translation of the data formats for input to the cryptogram algorithms may need to be performed by VisaNet or Issuer Host Systems as described in Appendix D, Authentication Keys and Algorithms.

E.2 Cryptogram Version 12

Cryptogram Version 12 has been made available to designate issuer proprietary cryptogram processing. It may be used by issuers that do not wish to support Cryptogram Version 10 in the early stages of migration.

CDOL1 and CDOL2 must be present in the card. The card must respond to the GENERATE APPLICATION CRYPTOGRAM (AC) command from the terminal in compliance with the EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0. The Derivation Key Index (DKI) can be defaulted to "0" (or any valid value) because the issuer does not intend to support key management or issuer host authentication processing immediately.

E.3 Cryptogram Version 14

Cryptogram Version 14 uses the optional cryptogram algorithm defined in the *EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0 (EMV 4.0), Book 2*, Section 8. It is offered as an option for issuers that wish to minimize use of the card's Unique Derivation Key (UDK). With Cryptogram Version 14, a 16-byte session key is generated with each transaction using the session key of the previous transaction and the Application Transaction Counter (ATC).

CDOL1 and CDOL2 must be present in the card. The data is input to the cryptogram in the same order and format used with Cryptogram Version 10. The data is padded into 8-byte data blocks as described in Step 3 of Section D.2 Generating the TC, AAC, and ARQC of this document.

Because the format of the data in the card may be different than the format of the data transmitted in authorization and clearing messages, translation of the data formats for input to the cryptogram algorithms may need to be performed by Issuer Host Systems as described in Appendix D, Authentication Keys and Algorithms.

Card Internal Security Architecture F

This appendix describes the Integrated Circuit Card's internal security framework. The use of the security framework is limited to those processes that are controlled by the card operating system and that affect any card data or executable code.

F.1 Objective of ICC Internal Security

The objective of this security framework is to ensure that appropriate security mechanisms are employed by the card operating system and to provide security and integrity for all data and processes within the card. This framework is designed to address access to data files and the use of commands and cryptographic algorithms.

F.2 Overview of ICC Internal Security

- The fundamental constructs of this security framework include two basic features:
- The establishment of a *security domain*
- The use of specific access conditions for every elementary file

F.2.1 Security Domain

Access to all data and executable resources (in other words, data files, records, commands, and cryptographic keys and algorithms) is controlled by the operating system, thus allowing the establishment of the security domain. This is achieved via the processing of the SELECT and the GET PROCESSING OPTIONS commands. These commands are used to establish the information representing the security domain and thus define, at any one point in time, the scope of what specific data and executable resources can be accessed.

Because that information is used by the card operating system to control access to data at the file level, an issuer needs to consider carefully how to aggregate data objects and data elements together in files. In other words, data accessible at the same level should be aggregated in a file with similar data, and conversely data with dissimilar access requirements should not be aggregated within the same file.

The processing of the SELECT command makes available to the card operating system information referred to as the Application Management Data (AMD), which specifies all data files, records, and executable resources that can be subsequently accessed or used.

The AMD presented to the operating system after the selection of an application determines those files and executable resources that the application may access. As required for the Visa Smart Debit/Credit application, Record 1 of SFI 1 shall be included in the AMD at this stage in transaction processing. The subsequent issuance of the GET PROCESSING OPTIONS command may cause the operating system to modify the security domain as necessary so that additional files and records may be referenced, since the GET PROCESSING OPTIONS command provides file and record numbers within the Application File Locator.

Since the processing of the SELECT and GET PROCESSING OPTIONS commands establishes the security domain, the issuer can limit the resources that can be accessed during a transaction by including or excluding these resources from the AMD and Application File Locator. If data files are not referenced in the AMD and Application File Locator, those data files cannot be accessed. If commands or cryptographic algorithms are not referenced in the AMD and Application File Locator, those commands and algorithms cannot be used within the scope of the current security domain. The initial state of the AMD as defined during personalization shall include only those data files that can be accessed during the processing of a transaction for that application.

The initial AMD established by the selection of an application is defined during personalization. Details of the AMD are described in the following sections.

F.2.2 Elementary File Access Conditions

Access to an elementary file occurs only after at least one issuance of a SELECT command and the establishment of a security domain. Once the security domain is established and a subsequent command to read (such as the READ RECORD command) or to update data (such as the UPDATE RECORD command) is transmitted to an elementary file, the access conditions noted for that elementary file in the File Control Parameters (FCP) of its File Control Information (FCI) are enforced. Details of the FCP are noted in Section F.4 File Control Parameters. The inclusion of secure messaging or the VERIFY command, or both, as an access condition as indicated here requires that these conditions be satisfied in order to perform the requested access.

The access conditions noted for an elementary file apply to all commands that provide external access to ICC data, such as the READ RECORD, GET DATA, PUT DATA, or UPDATE RECORD command.

F.3 File Control Information

The File Control Information (FCI) is attached to each Application Definition File (ADF) or Application Elementary File (AEF) and describes the characteristics of the file. It is created for each file during personalization.

The FCI of an ADF contains File Management Data (FMD), which may contain the AMD. The AMD defines the security domain of the application.

F.3.1 Application Management Data

The AMD is created during personalization to define the initial security domain of the application and may be stored in the FMD of the ADF.

F.3.1.1 Security Domain

The security domain as reflected by the application's AMD defines the following:

- Resources, AEFs and internal elementary files (for example, Personal Identification Numbers (PINs), keys, parameters) accessible within the scope of the application
- Commands that may be performed in the context of the application
- Relationship between the commands and the resources

The security domain is defined by those resources noted in the AMD. If a resource is not included in the AMD, it cannot be used by the application. The security domain is defined as local to the application; in other words, all the definitions for the security domain may differ from one application to the other.

Two types of resources are defined:

- Data resource (described in Section F.3.2 Data Resources)
- Executable code resource (described in Section F.3.3 Executable Code Resource)

In addition, a resource may be defined as "not yet assigned to the application" to allow further allocation of the resource to the application using the appropriate post-issuance command. The resources and their relationships are described in the AMD.

F.3.2 Data Resources

A data resource may be one of the following:

- Data file and its records
- Key
- PIN

F.3.2.1 Data Identification

Data resources are data elements that may be contained in files. A data resource is identified by a unique identifier internal to the ICC. Files are identified by a unique file identifier internal to the ICC. Data elements not contained in a file are identified by a unique data identifier to the ICC.

Any data resource necessary to run an application shall be identified in the AMD of the application.

For a file containing data elements that may be accessed using a command defined in the AMD (such as the READ RECORD or UPDATE RECORD command), the relationship between the SFI that is uniquely identified within an application and that can be externally referenced and the file identifier that is uniquely identified internal to the ICC and that can be internally referenced is maintained in the AMD.

For a data object not contained in a file and that may be accessed using a command defined in the AMD (such as the GET DATA command), the relationship between the data object's tag that can be externally referenced and the unique data identifier that is internal to the ICC and that can be internally referenced is maintained in the AMD.

F.3.2.2 Key Identification

Keys may be contained in files or may be independent data elements. Keys should never be referenced externally. For a key contained in a file, the AMD maintains the file identifier and the reference to the key necessary to locate it when using a command defined in the AMD and a cryptographic algorithm also defined in the AMD.

For a key not contained in a file, the AMD maintains the unique key identifier internal to the ICC necessary to locate it when using a command defined in the AMD and a cryptographic algorithm also defined in the AMD.

F.3.2.3 PIN/Password Identification

A PIN or a password may be contained in files or may be independent data elements. PINs and passwords shall be externally referenced only by using a command defined in the AMD in conjunction with secure messaging.

For a PIN or a password contained in a file, the AMD maintains the file identifier and the reference to the PIN or password necessary to locate it when using a command defined in the AMD and a cryptographic algorithm also defined in the AMD. For a PIN or a password not contained in a file, the AMD maintains the unique PIN or password identifier internal to the ICC necessary to locate it when using a command defined in the AMD and a cryptographic algorithm also defined in the AMD.

F.3.3 Executable Code Resource

An executable code resource may be one of the following:

- Command
- Cryptographic algorithm

F.3.3.1 Command Identification

A command resource includes CLA and INS bytes, which are used by the operating system to locate the command. The command resource entry includes attributes for the data that may be accessed using the command and, optionally, parameters related to keys and algorithms.

F.3.3.2 Algorithm Identification

An algorithm resource establishes the link between the algorithm identifier as defined for the application and the actual reference to the algorithm used by the operating system to locate the executable code.

F.4 File Control Parameters

Each elementary file contains a FCP in its FCI which contains additional information relative to the access conditions of the file. This information is placed in the ICC during personalization and is used by the ICC's operating system in conjunction with the AMD contained in the FCI of the ADF to build the security domain of the application. The access conditions available for an elementary file are shown in Table F–1.

Table F–1: Available Access Conditions for an Elementary File

Read	Update	Access Conditions
Yes/No	Yes/No	
Yes/No	Yes/No	Secure messaging
Yes/No	Yes/No	VERIFY
Not Applicable	Yes/No	Data encipherment

In Table F–1, the *Read* column refers to the use of a read command (such as the READ RECORD or GET DATA command) for accessing data within elementary files. The *Update* column refers to the use of an update command (such as the PUT DATA or UPDATE RECORD command) for accessing data within elementary files.

The FCP indicates whether data is conveyed in the Issuer Script Command UPDATE RECORD as either enciphered data or plaintext data.

The FCP may be used as a component for implementing the logical constructs of the AMD. In addition, the FCP describes the security access conditions that are enforced for an elementary file for any application on a card.

F.5 ICC Card Resident Data Recommended Access Conditions

The following are recommendations for data access conditions. These recommendations are applicable to data that may be accessed by the READ RECORD, UPDATE RECORD, or GET DATA commands or other similar proprietary commands.

- This recommendation addresses data that may be read by using the READ RECORD command: All tagged ICC-resident data that can be externally referenced should have read-only status without an access condition of secure messaging.
- This recommendation lists data that may be changed by using the PUT DATA command with secure messaging and that may be read using the GET DATA command:
  - Lower Consecutive Offline Limit (“9F58”)
  - Upper Consecutive Offline Limit (“9F59”)
  - Consecutive Transaction Limit (International—Country)
  - Consecutive Transaction Limit (International)
  - Cumulative Total Transaction Amount Limit
  - Cumulative Total Transaction Amount Limit (Dual Currency)
  - Cumulative Total Transaction Amount Upper Limit
  - Currency Conversion Factor
  - VLP Funds Limit
  - VLP Single Transaction Limit
- This recommendation lists data that may be updated by using the Visa proprietary PIN CHANGE/UNBLOCK command with secure messaging and that may not be read:
  - Reference PIN
- This recommendation lists data that may be read using the GET DATA command and that may be reset to a predetermined limit by using the PIN CHANGE/UNBLOCK command with secure messaging:
  - PIN Try Counter
- This recommendation lists data that may be read using the READ RECORD command and that may be updated by using UPDATE RECORD command with secure messaging:
  - Record 1, SFI 1

Card Requirements for Visa Low-Value Payment Feature G

The Visa Low-value Payment (VLP) feature of VSDC provides members with an option of pre-authorizing spending power on the card for use in offline low-value payments. If both the card and terminal support VLP and the VLP transaction criteria are satisfied, the transaction is a VLP transaction. The VLP transaction criteria include the Amount Authorized being less than the terminal's VLP Terminal Transaction Limit, the card's VLP Available Funds, and the card's VLP Single Transaction Limit.

Issuer-selected VLP risk management features may differ from those selected for non-VLP VSDC transactions. To limit the number of online authorizations for these low value transactions, standard VSDC velocity checking counters and accumulators are not incremented during VLP transactions.

VLP transactions are always approved or declined offline and are never sent online for authorization. The offline decision is based upon the results of the VLP risk management. Any requests requiring online authorization are processed subject to VSDC requirements and Visa and Visa Electron program rules.

The amount of spending power (VLP Available Funds) is automatically reset to the spending limit (VLP Funds Limit) after an online approved authorization when the issuer's Issuer Authentication requirements are satisfied.

The general requirements shall be implemented according to the EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0.

G.1 Card Data

Cards supporting VLP shall contain the first four data elements described in Table G–1. The VLP Single Transaction Limit is optional.

Table G–1: Initiate Application Processing—Card Data

Data Element	Description
Program Options Data Object List (PDOL)	Must contain the tags for VLP Terminal Support Indicator, Amount Authorized, and Transaction Currency Code
VLP Available Funds	An accumulator that is decremented by the transaction amount when a VLP transaction is approved.
VLP Funds Limit	Issuer limit for VLP Available Funds that is used by the card to reset VLP Available Funds after an online approved transaction.
VLP Issuer Authorization Code	Code on the card that indicates that the transaction is approved for VLP. It is placed in the Authorization Code in the clearing message if the transaction is approved offline. The format must be “VLPxxx” where xxx is any issuer-designated number.
VLP Single Transaction Limit	Maximum amount allowed for a single VLP transaction.

A card supporting VLP may have duplicate versions of the data described in Table G–2 for use during non-VLP and VLP transactions.

NOTE: *The Issuer may define other VLP specific data elements as needed. Data elements with duplicate tags should be stored in records and updated using UPDATE RECORD. Data elements updated with PUT DATA must have unique tags.*

Table G–2: Duplicate Data Elements for VLP

Data Element	Description
Application File Locator (AFL)	Indicates records related to the given application. For VLP transactions, these include a record containing the VLP Issuer Authorization Code and VLP Available Funds. The AFL may also designate other records which are different from those used for non-VLP transactions such as a record with a different Cardholder Verification Method (CVM) List.
Application Interchange Profile (AIP)	An AIP used for VLP transactions that indicates the card support for specific functions. An issuer may select different functions for VLP transactions than for non-VLP transactions.
CVM List	A separate CVM List is necessary if the Issuer wishes different cardholder verification to be performed for VLP transactions than for non-VLP transactions.
ICC PK Certificate	A separate ICC PK Certificate is necessary for VLP transactions if DDA is supported for VLP transactions and any of the signed data is different for VLP transactions.
Issuer Action Codes (IACs)	Separate IACs are necessary if the Issuer's conditions for offline declines, online processing, or offline decline (if online processing does not complete) differ from those used during non-VLP transactions.
Signed Static Application Data (SAD)	A separate SAD is necessary if SDA is supported for VLP transactions and any of the signed data is different for VLP transactions.

The card uses the VLP-related card data described in Table G–3 during VLP transactions.

Table G–3: Initiate Application Processing—Card Data

Data Element	Description
Application Currency Code “9F51”	Visa proprietary data element indicating the currency in which the account is managed according to International Organisation for Standardisation (ISO) 4217.

G.2 Terminal Data

The card uses the terminal card data described in Table G–4 during VLP transactions.

Table G–4: Initiate Application Processing—Terminal Data

Data Element	Description
Amount, Authorized	Authorized amount of the transaction (excluding adjustments)
Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217.
VLP Terminal Support Indicator	A data element that, if present in the terminal, indicates that the terminal supports VLP processing.
VLP Terminal Transaction Limit	The terminal uses this data element, if present, to determine whether a transaction can be processed as VLP. The Amount, Authorized must be below the VLP Terminal Transaction Limit, if present. If not present, the Amount, Authorized must be below the Terminal Floor Limit.

G.3 VLP Purchase Transaction Process

The following VLP-unique processing occurs during a purchase transaction involving a VLP card. Any processing not listed is the same for VLP and standard VSDC.

G.3.1 Application Selection

The terminal selects the VSDC application using the Visa or Visa Electron AID. The File Control Information (FCI) in the card response contains a PDOL requesting the VLP Terminal Support Indicator, Amount, Authorized, and Transaction Currency Code.

G.3.2 Initiate Application Processing

The terminal provides the VLP Terminal Support Indicator (set to "1") in the GET PROCESSING OPTIONS command if all the following conditions are satisfied:

- The terminal supports VLP
- The transaction is under the VLP Terminal Transaction Limit or the terminal Floor Limit if the terminal does not contain a separate VLP Terminal Transaction Limit.
- The terminal Transaction Type is purchase (does not indicate cash or cashback)

NOTE: *Terminals may optionally perform random selection processing and set the VLP Terminal Support Indicator to "0" if a transaction is selected. This will ensure VSDC processing for randomly selected transactions.*

Upon receiving the GET PROCESSING OPTIONS command, the card considers the transaction a VLP transaction when all of the following conditions are met:

- The GET PROCESSING OPTIONS command contains the VLP Terminal Support Indicator (set to "1")
- The Transaction Currency Code matches the Application Currency Code
- The Amount, Authorized is less than or equal to the VLP Available Funds
- The Amount, Authorized is less than or equal to the VLP Single Transaction Limit if present on the card
- The PIN Try Counter is not zero
- The Issuer Authentication Failure Indicator is 0.

If the card considers the transaction is a VLP transaction, the card shall:

- Decrement the VLP Available Funds by the Amount, Authorized.
- Return the GET PROCESSING OPTIONS response with an AIP that indicates the options supported for VLP transactions and with an AFL that designates the VLP-specific data and any VLP-unique data. The VLP-specific data consists of:
  - The VLP Issuer Authorization Code
  - The VLP Available Funds

If any of the conditions are not met, the transaction is not a VLP transaction, and the card returns the non-VLP VSDC AIP and AFL in the GET PROCESSING OPTIONS response. The terminal processes the transaction as a non-VLP VSDC transaction.

G.3.3 Card Action Analysis

For transactions designated as VLP during Initiate Application Processing, the card performs the following steps:

- If the terminal declines the transaction offline (requests an AAC), the card increments the VLP Available Funds by the Amount, Authorized to reverse the decrement done during Initiate Application Processing.
- The VSDC velocity checks, Online Authorization Not Completed check, and New Card check are bypassed.
- Standard VSDC velocity related counters and accumulators are *not* incremented.
- The terminal should never request online processing. If the card receives an online processing request (an ARQC request in the first GENERATE AC), the card shall return an offline decline in the GENERATE AC response.

G.3.4 Online Processing

Online processing is not supported for VLP transactions.

G.3.5 Completion

Because VLP transactions are offline, the card does not perform Completion processing.

G.4 VLP Reset Transaction Processing

Reset of the VLP Available Funds to the VLP Funds Limit occurs after an online authorization or status check at a point-of-service (POS) device or ATM or after a status check at a dedicated online unattended terminal.

A VLP card shall automatically reset the VLP Available Funds to the VLP Funds Limit during Completion after a VSDC online approval if Issuer Authentication was either (1) successful, (2) optional and not performed, or (3) not supported.

G.5 Updating the VLP Limits

The issuer may change the VLP Funds Limit or the VLP Single Transaction Limit using a PUT DATA Issuer Script Command. The script commands must satisfy the requirements specified in Chapter 14, Issuer-to-Card Script Processing, including all requirements associated with secure messaging.

G.6 VLP Transaction Flow

The flow in Table G–1 and Table G–2 illustrates processing which is unique to VLP. Processing which is the same as for non-VLP transactions is not shown.

Figure G–1: VLP Transaction Flow (1 of 2)

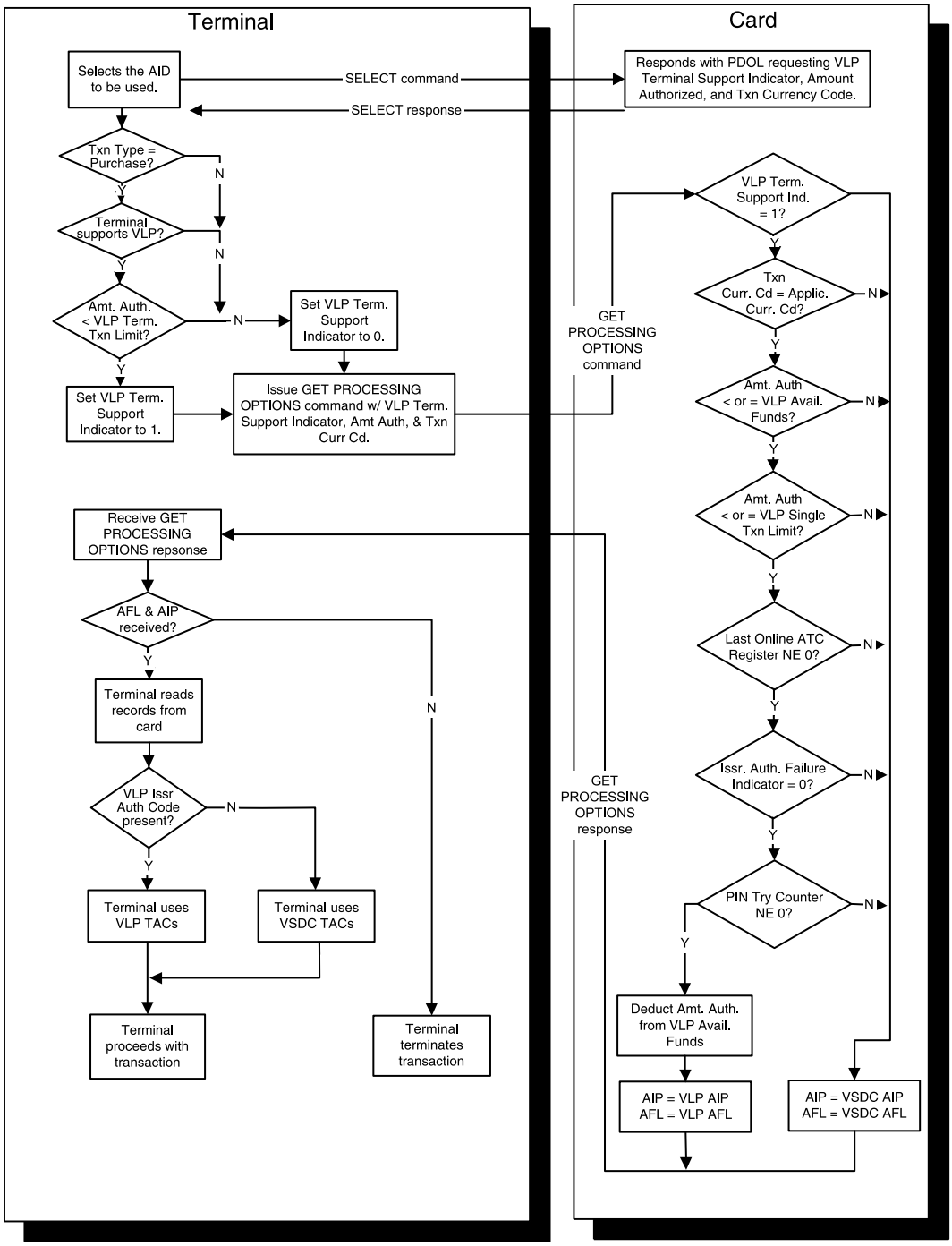
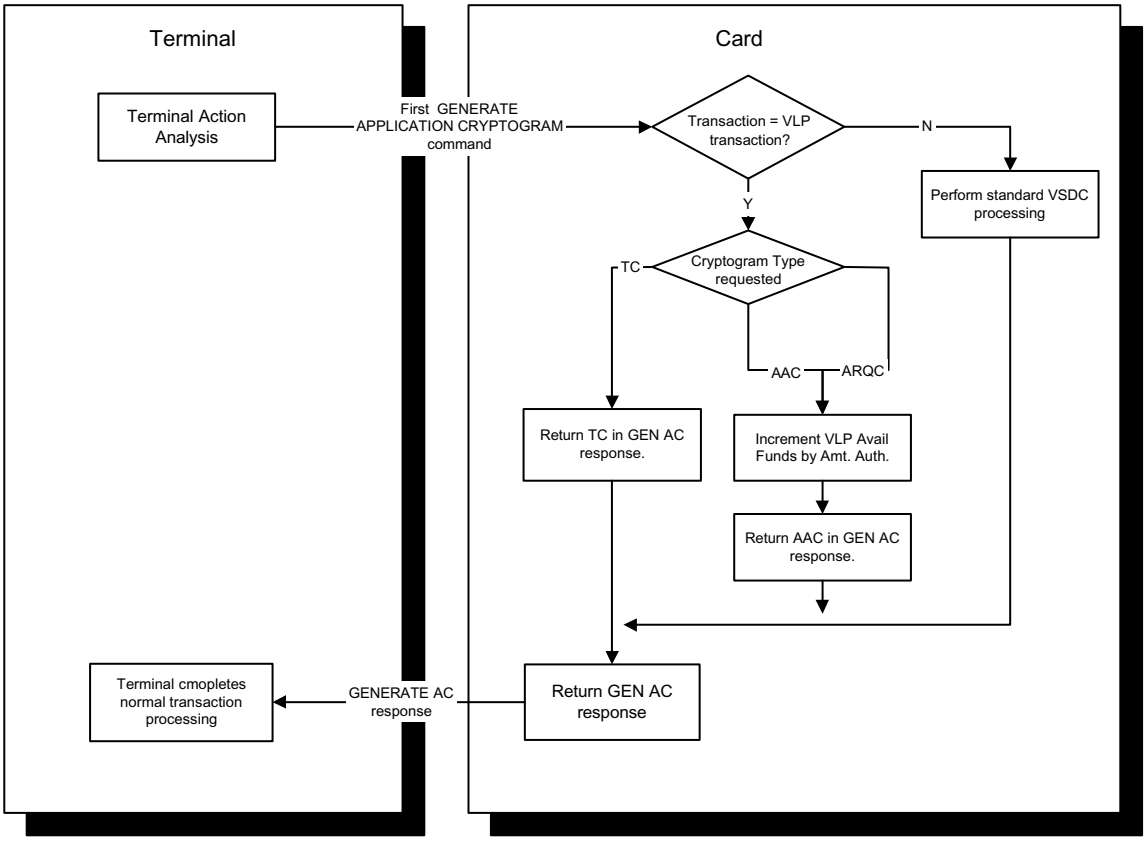


Figure G–2: VLP Transaction Flow (2 of 2)



Acronyms H

Table H–1: Acronyms (1 of 6)

Acronym	Meaning
a	alpha
AAC	Application Authentication Cryptogram
AAR	Application Authentication Referral
AC	Application Cryptogram
ADA	Application Default Action
ADF	Application Definition File
AEF	Application Elementary File
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
AMD	Application Management Data
an	alphanumeric

Table H–1: Acronyms (2 of 6)

Acronym	Meaning
ans	alphanumeric special
APDU	Application Protocol Data Unit
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
ATM	Automated Teller Machine
AUC	Application Usage Control
Auth.	authentication
b	binary
BIN	BASE Identification Number
C	conditional
CA	Certificate Authority
CAM	Card Authentication Method
CDOL	Card Risk Management Data Object List
Cert.	certificate
CID	Cryptogram Information Data
CLA	Class Byte of the Command Message
cn	compressed numeric
Cons.	consecutive
CPLC	Card Production Life Cycle Data
Cum.	cumulative

Table H–1: Acronyms (3 of 6)

Acronym	Meaning
CVM	Cardholder Verification Method
CVR	Card Verification Results
CVV	Card Verification Value
DDA	Dynamic Data Authentication
DDF	Directory Definition File
DDOL	Dynamic Data Authentication Data Object List
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DF	dedicated file
EEPROM	Electronically Erasable Programmable Read-Only Memory
EMV	Europay, MasterCard, Visa
ENC MDK	Master Data Encipherment DEA Key
ENC UDK	Unique Data Encipherment DEA Key
FCI	File Control Information
FCP	File Control Parameters
FMD	File Management Data
GPO	GET PROCESSING OPTIONS
hex.	hexadecimal
HHMMSS	hours, minutes, seconds
HSM	host security module
IA	Issuer Authentication

Table H–1: Acronyms (4 of 6)

Acronym	Meaning
IAC	Issuer Action Code
IC	integrated circuit
ICC	integrated circuit card
IEC	International Electrotechnical Commission
IFD	interface device
INS	Instruction Byte of the Command Message
Int'l	international
ISO	International Organisation for Standardisation
Lc	Length of the Command Data Field
Le	Expected Length of the Response Data Field
L_D	Length of the plaintext data in the Command Data Field
LRC	Longitudinal Redundancy Check
M	mandatory
MAC	Message Authentication Code
MAC MDK	Master Message Authentication Code DEA Key
MAC UDK	Unique Message Authentication Code DEA Key
MCC	Merchant Category Code
MDK	Master DEA Key
n	numeric
N/A	not applicable
N_{CA}	Length of the Certification Authority Public Key Modulus

Table H–1: Acronyms (5 of 6)

Acronym	Meaning
N_I	Length of the Issuer Public Key Modulus
N_{IC}	Length of the ICC Public Key Modulus
No.	number
O	optional
P1	Parameter 1
P2	Parameter 2
PAN	Primary Account Number
PDOL	Processing Options Data Object List
PIN	Personal Identification Number
PIX	Proprietary Application Identifier Extension
PK	public key
PKI	Certificate Authority Public Key Index
POS	point of service
PSE	payment system environment
PVV	PIN Verification Value
R	required
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
ROM	Read-Only Memory
RSA	Rivest, Shamir, Adleman
SAD	Signed Static Application Data

Table H–1: Acronyms (6 of 6)

Acronym	Meaning
SAM	Secure Access Module
SDA	Static Data Authentication
SFI	Short File Identifier
SW1, SW2	Status Words
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
TLV	tag-length-value
Txn.	transaction
TSI	Transaction Status Information
TVR	Terminal Verification Results
UDK	Unique DEA Key
var.	variable
V.I.P.	VisaNet Integrated Payment
VLP	Visa Low-value Payment
YDDD	year, day where Y = right-most digit of the year (0–9) and DDD = Julian day of the year (001–366)
YYMM	year, month where YY = year (00–99) and MM = month (01–12)
YYMMDD	year, month, day where DD = day (01–31)

Glossary

This is a glossary of terms used in this specification; it is not intended as a data dictionary. For descriptions of terminal and acquirer data elements, refer to Appendix A of the Card and Terminal volumes of this specification.

acquirer

A Visa member that signs a merchant or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction into interchange.

ANSI

American National Standards Institute. A U.S. standards accreditation organization.

application

A computer program and associated data that reside on an integrated circuit chip and satisfy a business function. Examples of applications include payment, stored value, and loyalty.

Application Authentication Cryptogram (AAC)

A cryptogram generated by the card for offline and online declined transactions.

application block

Instructions sent to the card by the issuer, to shut down the selected application on a card to prevent further use of that application. This process does not preclude the use of other applications on the card.

ATM

An unattended terminal that has electronic capability, accepts PINs, and disburses currency or cheques.

ATM cash disbursement

A cash disbursement obtained at an ATM displaying the Visa, PLUS, or Visa Electron acceptance mark, for which the cardholder's PIN is accepted.

authentication

A cryptographic process that validates the identity and integrity of data.

authorization

A process where an issuer or a representative of the issuer approves a transaction.

authorization controls

Information in the chip application enabling the card to act on the issuer's behalf at the point of transaction. The controls help issuers manage their below-floor-limit exposure to fraud and credit losses. Also known as offline authorization controls.

authorization request

A merchant's or acquirer's request for an authorization.

Authorization Request Cryptogram (ARQC)

The cryptogram generated by the card for transactions requiring online authorization and sent to the issuer in the authorization request. The issuer validates the ARQC during the Online Card Authentication (CAM) process to ensure that the card is authentic and was not created using skimmed data.

authorization response

The issuer's reply to an authorization request. Types of authorization responses are:

- approval
- decline
- pickup
- referral

Authorization Response Cryptogram (ARPC)

A cryptogram generated by the issuer and sent to the card in the authorization response. This cryptogram is the result of the Authorization Request Cryptogram (ARQC) and the Issuer's authorization response encrypted with the Unique Derivation Key (UDK). It is validated by the card during Issuer Authentication to ensure that the response came from a valid issuer.

Bank Identification Number (BIN)

A 6-digit number assigned by Visa and used to identify a member or processor for authorization, clearing, or settlement processing.

BASE I Authorization System

The V.I.P. System component that performs message routing, cardholder and card verification, and related functions such as reporting and file maintenance.

BASE II

The VisaNet system that provides deferred clearing and settlement services to members.

byte

8 bits of data.

card acceptance device

A device capable of reading and/or processing a magnetic stripe or chip on a card for the purpose of performing a service such as obtaining an authorization or processing a payment.

card authentication

A means of validating whether a card used in a transaction is the genuine card issued by the issuer.

Card Authentication Method (CAM)

See Online Card Authentication.

card block

Instructions, sent to the card by the Issuer, which shut down all proprietary and non-proprietary applications that reside on a card to prevent further use of the card.

Card Verification Value (CVV)

A unique check value encoded on a card's magnetic stripe and chip to validate card information during an online authorization.

cardholder

An individual to whom a card is issued or who is authorized to use that card.

cardholder verification

The process of determining that the presenter of the card is the valid cardholder.

Cardholder Verification Method (CVM)

A method used to confirm the identity of a cardholder.

cash disbursement

Currency, including travelers cheques, paid to a cardholder using a card.

cashback

Cash obtained in conjunction with, and processed as, a purchase transaction.

CCPS

Chip Card Payment Service, the former name for Visa Smart Debit and Visa Smart Credit (VSDC).

Certificate Authority (CA)

A trusted central administration that issues and revokes certificates.

chargeback

A transaction that an issuer returns to an acquirer.

chip

An electronic component designed to perform processing or memory functions.

chip-capable

A card acceptance device that is designed and constructed to facilitate the addition of a chip reader/writer.

chip card

A card embedded with a chip that communicates information to a point-of-transaction terminal.

clearing

The collection and delivery to the issuer of a completed transaction record from an acquirer.

cleartext

See plaintext.

cryptogram

A numeric value that is the result of data elements entered into an algorithm and then encrypted. Commonly used to validate data integrity.

cryptographic key

The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt or decrypt a message.

cryptography

The art or science of keeping messages secret or secure, or both.

CVM List

An issuer-defined list contained within a chip application establishing the hierarchy of methods for verifying the authenticity of a cardholder.

data authentication

Validation that data stored in the integrated circuit card has not been altered since card issuance. *See also* Offline Data Authentication.

Data Encryption Algorithm (DEA)

An encipherment operation and an inverse decipherment operation in a cryptographic system.

Data Encryption Standard (DES)

The public domain symmetric key cryptography algorithm of the National Institute for Standards and Technology.

decryption

The process of transforming ciphertext into cleartext.

DES key

A secret parameter of the Data Encryption Standard algorithm.

digital signature

A cryptogram generated by encrypting a message digest (or hash) with a private key that allows the message content and the sender of the message to be verified.

double-length DES Key

Two secret 64-bit input parameters each of the Data Encryption Standard algorithm, consisting of 56 bits that must be independent and random, and 8 error-detecting bits set to make the parity of each 8-bit byte of the key odd.

Dynamic Data Authentication (DDA)

A type of Offline Data Authentication where the card generates a cryptographic value using transaction-specific data elements for validation by the terminal to protect against skimming.

Easy Entry

A replication of the magnetic stripe information on the chip to facilitate payment as part of multi-application programs. Easy Entry is not EMV-compliant and is being phased out.

EMV specifications

Technical specifications developed jointly by Europay International, MasterCard International, and Visa International to create standards and ensure global interoperability for use of chip technology in the payment industry.

encryption

The process of transforming cleartext into ciphertext.

expired card

A card on which the embossed, encoded, or printed expiration date has passed.

floor limit

A currency amount that Visa has established for single transactions at specific types of merchants, above which online authorization is required.

Hardware Security Module (HSM)

A secure module used to store cryptographic keys and perform cryptographic functions.

hash

The result of a non-cryptographic operation, which produces a unique value from a data stream.

host data capture system

An acquirer authorization system that retains authorized transactions for settlement without notification from the terminal that the transaction was completed.

Integrated Circuit Card (ICC)

See chip card.

Integrated Circuit Chip

See chip.

interchange

The exchange of clearing records between members.

International Organisation for Standardisation (ISO)

The specialized international agency that establishes and publishes international technical standards.

interoperability

The ability of all card acceptance devices and terminals to accept and read all chip cards that are properly programmed.

issuer

A Visa member that issues Visa or Electron cards, or proprietary cards bearing the PLUS or Visa Electron Symbol.

Issuer Action Codes (IACs)

Card-based rules which the terminal uses to determine whether a transaction should be declined offline, sent online for an authorization, or declined if online is not available.

Issuer Authentication

Validation of the issuer by the card to ensure the integrity of the authorization response. *See* Authorization Response Cryptogram (ARPC).

key generation

The creation of a new key for subsequent use.

key management

The handling of cryptographic keys and other related security parameters during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

magnetic stripe

The stripe on the back of the card that contains the magnetically coded account information necessary to complete a non-chip electronic transaction.

Magnetic Stripe Image

The minimum chip payment service data replicating information in the magnetic stripe required to process a transaction that is compliant with EMV.

Master Derivation Keys (MDK)

Master DES keys stored in the issuer host system. These keys are used to generate Unique Derivation Keys (UDKs) for personalization, to validate ARQCs, and to generate ARPCs.

Merchant Category Code (MCC)

A code designating the principal trade, profession, or line of business in which a merchant is engaged.

message authentication code (MAC)

A digital code generated using a cryptographic algorithm which establishes that the contents of a message have not been changed and that the message was generated by an authorized entity.

multi-application

The presence of multiple applications on a chip card (for example, payment, loyalty, and identification).

nibble

The four most significant or least significant bits of a byte of data.

offline approval

A transaction that is positively completed at the point of transaction between the card and terminal without an authorization request to the issuer.

offline authorization

A method of processing a transaction without sending the transaction online to the issuer for authorization.

offline-capable

A card acceptance device that is able to perform offline approvals.

Offline Data Authentication

A process whereby the card is validated at the point of transaction using RSA public key technology to protect against counterfeit or skimming. VIS includes two forms: Static Data Authentication (SDA) and Dynamic Data Authentication (DDA).

offline decline

A transaction that is negatively completed at the point of transaction between the card and terminal without an authorization request to the issuer.

offline-only terminal

A card acceptance device that is not capable of sending transactions online for issuer authorization.

offline PIN

A PIN value stored on the card that is validated at the point of transaction between the card and the terminal.

offline PIN verification

The process whereby a cardholder-entered PIN is passed to the card for comparison to a PIN value stored secretly on the card.

online authorization

A method of requesting an authorization through a communications network other than voice to an issuer or issuer representative.

online-capable terminal

A card acceptance device that is able to send transactions online to the issuer for authorization.

Online Card Authentication (CAM)

Validation of the card by the issuer to protect against data manipulation and skimming. *See* Authorization Request Cryptogram (ARQC).

online PIN

A method of PIN verification where the PIN entered by the cardholder into the terminal PIN pad is DES-encrypted and included in the online authorization request message sent to the issuer.

personalization

The process of populating a card with the application data that makes it ready for use.

plaintext

Data in its original unencrypted form.

point of transaction (POT)

The physical location where a merchant or acquirer (in a face-to-face environment) or an unattended terminal (in an unattended environment) completes a transaction.

point-of-transaction terminal

A device used at the point of transaction that has a corresponding point-of-transaction capability. *See also* Card Acceptance Device.

post-issuance update

A command sent by the issuer through the terminal via an authorization response to update the electronically stored contents of a chip card.

private key

As part of an asymmetric cryptographic system, the key that is kept secret and known only to the owner.

public key

As part of an asymmetric cryptographic system, the key known to all parties.

public key cryptographic algorithm

A cryptographic algorithm that allows the secure exchange of information, but does not require a shared secret key, through the use of two related keys—a public key which may be distributed in the clear and a private key which is kept secret.

public key pair

The two mathematically related keys, a public key and a private key which, when used with the appropriate public key cryptographic algorithm, can allow the secure exchange of information, without the secure exchange of a secret.

purchase transaction

A retail purchase of goods or services; a point-of-sale transaction.

quasi-cash transaction

A transaction representing a merchant's sale of items, such as gaming chips or money orders, that are directly convertible to cash.

random selection

An EMV online-capable terminal function that allows for the selection of transactions for online processing. Part of Terminal Risk Management.

receipt

A paper record of a transaction generated for the cardholder at the point of transaction.

referral response

An authorization response where the merchant or acquirer is instructed to contact the issuer for further instructions before completing the transaction.

reversal

A BASE II or online financial transaction used to negate or cancel a transaction that has been sent through interchange.

ROM (Read-Only Memory)

Permanent memory that cannot be changed once it is created. It is used to store chip operating systems and permanent data.

RSA (Rivest, Shamir, Adleman)

A public key cryptosystem developed by Rivest, Shamir, and Adleman, used for data encryption and authentication.

secret key

A key that is used in a symmetric cryptographic algorithm (that is, DES), and cannot be disclosed publicly without compromising the security of the system. This is not the same as the private key in a public/private key pair.

secure messaging

A process that enables messages to be sent from one entity to another, and protects against unauthorized modification or viewing.

session key

A temporary cryptographic key computed in volatile memory and not valid after a session is ended.

settlement

The reporting of settlement amounts owed by one member to another or to Visa, as a result of clearing.

Single Message System

A component of the V.I.P. System that processes Online Financial and Deferred Clearing transactions.

smart card

A commonly used term for a chip card.

Static Data Authentication (SDA)

A type of Offline Data Authentication where the terminal validates a cryptographic value placed on the card during personalization. This validation protects against some types of counterfeit, but does not protect against skimming.

Terminal Action Codes (TACs)

Visa-defined rules in the terminal which the terminal uses to determine whether a transaction should be declined offline, sent online for an authorization, or declined if online is not available.

transaction

An exchange of information between a cardholder and a merchant or an acquirer that results in the completion of a financial transaction.

Triple DES

The data encryption algorithm used with a double-length DES key.

V.I.P. System

VisaNet Integrated Payment System, the online processing component of VisaNet.

Visa Certificate Authority (CA)

A Visa-approved organization certified to issue certificates to participants in a Visa payment service.

Visa Low-value Payment (VLP)

VLP is a feature of VSDC designed to provide an optional source of pre-authorized spending power that is reserved for rapid processing of offline low-value payments.

Visa Smart Debit and Visa Smart Credit (VSDC)

The Visa service offerings for chip-based debit and credit programs. These services, based on EMV and VIS specifications, are supported by VisaNet processing, as well as by Visa rules and regulations.

VisaNet

The systems and services, including the V.I.P. and BASE II systems, through which Visa delivers online financial processing, authorization, clearing, and settlement services to members.

Index

A

AAC, 11–2, 11–16, 13–5, 13–9, 13–13, 13–15, 13–17, 14–9, C–4, D–1, D–4, D–10, E–1

AAR, C–4

ADF. *See* Application Definition File

advice message, 11–3, 11–17, 13–14, 13–18

AID, 3–2, 3–5

Amount X, 8–3

Amount Y, 8–3

Amount, Authorized, 9–3, 11–2, 11–5, 11–12, 11–18, 13–6, 13–18, D–3, E–2, G–1 to G–2, G–4 to G–5

Amount, Other, D–3, E–2

APPLICATION BLOCK command, 2–10, 14–9, C–1 to C–2

application blocking, 8–6, 8–12

Application Cryptogram, 6–10, 10–4, 11–2, 11–6, 11–17, 11–19, 12–2, 13–5, 13–7, 13–10, 13–13 to 13–14, 13–18, B–3, D–4, D–13, E–1

Application Currency Code, 8–2, 11–2 to 11–3, 11–11 to 11–13, 11–17 to 11–18, 13–3, 13–18, C–6, G–4 to G–5

Application Default Action, 8–12, 11–2, 11–7, 11–9, 11–15, 11–17, 13–3, 13–11, 13–14 to 13–15, C–6

Application Definition File, 3–2, A–45, F–3

Application Effective Date, 6–8, 7–2, 7–5

Application Elementary Files, 3–3, 5–2, F–3

Application Expiration Date, 6–8, 7–2, 7–6

Application File Locator, 4–1 to 4–2, 4–4, 5–2, 6–10, F–2, G–3, G–6

Application Interchange Profile, 4–1 to 4–2, 4–4, 6–6, 6–8, 8–2, 11–2, 11–9, 12–3, 12–6, 13–3, 13–11, 15–3, D–3, E–2, G–3, G–6

Application Label, 3–2 to 3–3, C–15

Application Management Data, F–2 to F–4, F–6

Application PAN Sequence Number, 6–8

Application Preferred Name, 3–2 to 3–3, C–14

Application Priority Indicator, 3–2 to 3–3, C–15

Application Selection, 1–8, 2–1, 2–8, 3–1, 4–4, 4–7, 14–10, G–5

- card data, 3–2
- commands, 3–6
- functions, 3–1
- identifying and selecting the application, 3–11
- processing flow, 3–12
- terminal data, 3–5

Application Selection Indicator, 3–5

APPLICATION UNBLOCK command, 2–10, 14–10, C–1, C–3

Application Usage Control, 2–3, 6–8, 7–2, 7–4

Application Version Number, 7–3

Application Version Number (“9F08”), 7–2

Application Version Number (“9F09”), 7–3

applications, multiple Visa on single card, 3–2

ARPC, 12–4, 12–6, 13–11, C–3, D–6, D–10, D–13

ARQC, 11–2, 11–16, 11–18 to 11–19, 12–2 to 12–3, 12–5, 13–5, C–4, D–1, D–4, D–10, E–1

ATC, 4–2, 4–5, 6–11, 9–2, 9–4 to 9–5, 11–11, 12–2, 13–5, 13–7, 13–15, 14–7, B–3, B–8, C–7, D–3, E–2 to E–3

ATM, 1–7, 7–4

authorization message, C–4

Authorization Response Code, 12–4, 12–6, 13–6, 13–9, C–3

Authorization Response Message, 14–13

authorization response message, C–2

B

backup, data element, A–44

biometrics, 8–1

C

candidate list, building the, 3–7 to 3–8
Card Action Analysis, 2–4, 2–9, 6–16 to 6–17, 8–14, 10–5, 11–1, 12–3, 12–7, 12–9, 13–25, 14–17
  card data, 11–2, 11–5
  processing, 11–6
  terminal data, 11–5, 13–7
CARD BLOCK command, 2–10, 14–10, C–1, C–3
card data
  for Application Selection, 3–2
  for Card Action Analysis, 11–2
  for Cardholder Verification, 8–2
  for Completion, 13–3
  for Dynamic Data Authentication, 6–11
  for Initiate Application Processing, 4–2 to 4–3
  for Issuer-to-Card Script Processing, 14–7
  for Online Processing, 12–2
  for Processing Restrictions, 7–2
  for Read Application Data, 5–2
  for Static Data Authentication, 6–7
  for Terminal Action Analysis, 10–2
  for Terminal Risk Management, 9–2
Card Declined Transaction Offline, 11–17
Card Internal Security Architecture, F–1
Card Production Life Cycle data, 14–10
Card Provides Response Cryptogram, 11–16
card reader, 8–9
Card Risk Management, 11–5, 11–19, 13–15
Card Risk Management checks, 11–7
Card Risk Management Data Object List. *See* CDOL1
Card Verification Value. *See* CVV
cardholder confirmation, 3–11
cardholder selection, 3–11
Cardholder Verification, 2–3, 2–8, 4–7, 8–1, 15–3
  card data, 8–2
  commands, 8–8
  processing, 8–9
  terminal data, 8–8
Cardholder Verification Method List. *See* CVM List
Cardholder Verification Value. *See* CVV
CDOL1, 10–3, 11–2, 11–5, D–2, D–4
CDOL2, 13–6 to 13–7, D–2, D–4
Certificate Authority Public Key Index, 6–4, 6–7, 6–9, 6–14, 8–7
Certificate Expiration Date, 6–4
CID. *See* Cryptogram Information Data
clearing message, C–4
Combined DDA/AC Generation, 1–8 to 1–9, 2–2, 2–8, 6–10, 6–13, 6–16, 11–19, 13–18
Command Identification, F–5
command support requirements, 2–10
commands, B–9, C–1, F–3, F–5
  APPLICATION BLOCK, 14–9, C–2
  APPLICATION UNBLOCK, 14–10, C–3
  CARD BLOCK, 14–10, C–3
  Cardholder Verification, 8–8
  EXTERNAL AUTHENTICATE, 12–5, C–3
  GENERATE AC, 11–2, 11–16, C–4
  GET CHALLENGE, C–4
  GET DATA, 9–4, C–5
  GET PROCESSING OPTIONS, 4–4, C–8
  INTERNAL AUTHENTICATE, 6–13, C–8
  PIN CHANGE/UNBLOCK, 14–11, C–8
  PUT DATA, 14–12, C–11
  READ RECORD, C–14
  SELECT, C–14
  UPDATE RECORD, 14–12, C–16
  VERIFY, C–18
Common Personalization for VSDC, 15–2
Completion, 2–6, 2–9, 6–12, 6–17, 8–15, 11–9, 11–26, 12–6 to 12–7, 12–9, 13–1, 14–17, G–6
  card data, 13–3
  processing flow, 13–8
  terminal data, 13–6
  transaction flow example, 13–20
conditional, A–44
confidentiality, B–1, B–5, C–2
Consecutive Offline Limit (“9F58”), C–11
Consecutive Transaction Counter (International), 11–3, 11–8, 11–11, 11–17 to 11–18, 13–3, 13–13, 13–18
Consecutive Transaction Counter (International—Country), 11–3, 11–8, 11–11, 11–17 to 11–18, 13–3, 13–13, 13–18
Consecutive Transaction Limit (International), 11–3, 11–11, 14–12, C–6, C–11, F–7
Consecutive Transaction Limit (International—Country), 11–3, 11–11, 14–12, C–6, C–11, F–7
counters, 13–1, 13–12, A–65
credit risk, 9–1
cryptogram, D–13
Cryptogram Information Data, 4–2, 4–5, 6–10, 11–3, 11–6, 11–17, 11–19, 12–2, 13–5, 13–7, 13–10, 13–12 to 13–13, 13–18
cryptogram version 10, D–2, D–4 to D–6, E–1 to E–2
cryptogram version 12, 15–3, D–2, E–1, E–3
cryptogram version 14, 1–9, D–2, D–4 to D–6, E–1, E–3
Cryptogram Version Number, 12–2, D–2, E–1
Cumulative Total Transaction Amount, 11–3, 11–12, 11–18, 13–3, 13–13, 13–16, 13–18

Cumulative Total Transaction Amount (Dual Currency), 11–3, 11–13, 11–18, 13–3, 13–13, 13–16, 13–18
Cumulative Total Transaction Amount Limit, 11–3, 11–12, 14–12, C–6, C–11, F–7
Cumulative Total Transaction Amount Limit (Dual Currency), 11–3, 11–13, 14–12, C–6, C–11, F–7
Cumulative Total Transaction Amount Upper Limit, 1–9, 13–3, 13–16, 14–12, C–6, C–11, F–7
Currency Conversion Factor, 11–4, 11–13, 11–18, 13–4, 14–12, C–6, C–11, F–7
CVM Code, 8–3
CVM Conditions, 8–3
CVM List, 1–7 to 1–8, 2–3, 4–4, 6–8, 8–1, 8–3, 8–9, G–3
CVM List processing card data, 8–2
CVM Type, 8–3
CVR, 4–2, 4–5, 6–9, 6–12, 8–6, 8–9, 8–11, 8–14, 11–3, 11–7, 11–16, 12–2 to 12–3, 13–7, 13–10, 14–7, D–3, E–2

D

Data Authentication Code (DAC), 1–7
data confidentiality, 14–14
Data encipherment, C–2
Data Encipherment Session Key, 14–5, 14–14, B–5, B–8, C–9
DDA, 2–2, 5–1, 6–1, 6–10 to 6–11, 11–7, 13–4
  terminal data, 6–13, 11–2, 11–10
DDA Failed on Last Transaction, 11–7, 11–10
DDA Failure Indicator, 6–12, 11–4, 11–10, 11–17, 13–10, 13–13, 13–17
DDOL, 6–11, 6–13
default CVM, 2–3
Default DDOL, 6–13
Derivation Key Index, 12–2, 15–3, E–3
DES, 10–4, D–5
DES cryptogram, 11–17
DF Name, 3–2, C–14
Directory Definition File, 3–3, 3–7, A–45
Directory File, 3–3
Directory Selection Method, 1–7, 3–7, 3–12
domestic, 4–4, 7–4 to 7–5
Dynamic Data Authentication Failure Indicator, 13–4
dynamic data elements, A–45
dynamic signature, 6–15, 11–19

E

elementary file, F–3
EMV, 1–1, 1–3, 1–7, 6–3
EMV documentation, 1–11
ENC MDK, 14–5, C–9, D–14
ENC UDK, B–5, B–8, C–9, D–14
Executable Code Resource, F–5
EXTERNAL AUTHENTICATE command, 2–10, 12–4 to 12–6, 13–9, 13–13, C–1, C–3

F

FCI Issuer Discretionary Data, 3–2, C–14
FCI Proprietary Template, C–14
FCI Template, C–14
FCP, F–3, F–6
File Control Information, 3–4, 3–7, B–2, C–14, F–3, F–6
floor limits, 9–4, G–5
FMD, F–3
fraud risk, 9–1
functional overview, 2–1
functions
  Card Action Analysis, 11–1
  Cardholder Verification, 8–1
  Completion, 13–1
  Initiate Application Processing, 4–1
  Offline Data Authentication, 6–1
  Online Processing, 12–1
  Processing Restrictions, 7–1
  Read Application Data, 5–1
  Terminal Action Analysis, 10–1
  Terminal Risk Management, 9–1
functions, mandatory and optional, 2–8

G

GENERATE AC command, 2–10, 6–10, 6–13, 6–16, 10–4, 11–6, 11–16, 12–5, 12–7, 13–5, 13–7, 13–10, 13–17 to 13–18, 14–7, 14–9, 14–13, 14–15, C–1, C–4, D–2, D–4, E–3
  Card Action Analysis, 11–6
  Terminal Action Analysis, 11–17
Geographic Indicator, 4–2, 4–4, C–6
Geographic Restrictions, 4–4
GET CHALLENGE command, 2–10, 8–8, 8–10, C–1, C–4
GET DATA command, 2–10, 8–8 to 8–9, 9–4, 14–10, C–1, C–5, F–4, F–7
GET PROCESSING OPTIONS command, 2–10, 4–1, 4–4, C–1, C–8, F–2, G–5

H

hash, 6–5, 6–10, 6–14
host security module, 6–4, D–12, D–14

I

IACs, 6–8, 10–2, 10–4, G–3
ICC Dynamic Data, 6–11, 6–15, 11–19
ICC Dynamic Number, 1–7

ICC key data, 6–3, 6–5, 8–7, D–14
ICC PIN Encipherment key data, 8–7
ICC PIN Encipherment PK Certificate, 8–7, D–14
ICC PIN Encipherment Private Key, 8–7, 8–11
ICC PIN Encipherment Public Key Exponent, 8–7
ICC PIN Encipherment Public Key Remainder, 8–7
ICC PK Certificate, 6–11, 6–14, 8–7, 10–2, D–14, G–3
ICC Private Key, 6–5, 6–12 to 6–13, 8–7, 8–11, 11–19
ICC Public Key, 1–9, 2–2, 6–5, 6–14
ICC Public Key Exponent, 6–11, 8–7
ICC Public Key Remainder, 6–12, 8–7
Identifying and Selecting the Application
  Application Selection, 3–11
indicators, 13–1, 13–12, A–65
Initiate Application Processing, 2–2, 2–8, 3–14 to 4–1, 5–3, 8–14, 12–9, G–5
  card data, 4–2 to 4–3, G–4
  processing, 4–4
  processing flow, 4–6
  terminal data, G–4
Interlink, 3–2 to 3–3
INTERNAL AUTHENTICATE command, 2–10, 6–10, 6–13, 6–15, C–1, C–8
international, 4–4, 7–4 to 7–5, 11–11
ISO documentation, 1–10
Issuer Application Data, 6–11, 11–3, 12–2, 13–5, C–4
issuer approval, 13–9, 13–11
Issuer Authentication, 2–5, 6–12, 11–9, 11–15, 12–1, 12–3, 12–6, 13–1, 13–10 to 13–12, 14–14, B–1, D–10, G–7
Issuer Authentication Data, 12–4
Issuer Authentication Failure Indicator, 11–4, 11–9, 12–3, 12–6, 13–4, 13–10, 13–12, G–5
Issuer Authentication Failure on Last Transaction, 11–7, 11–9
Issuer Authentication Indicator, 11–4, 11–9, 13–4, 13–11, C–6
Issuer Code Table Index, 3–2, 3–4, C–14
Issuer Country Code, 4–3 to 4–4, 6–8, 7–4, 11–3 to 11–4, 11–11, 11–17 to 11–18, 13–3 to 13–4, 13–18, C–7
Issuer Country Code “5F28”, 7–2
issuer decline, 13–9
Issuer Discretionary Data, 12–2, 13–7
issuer host, 12–1, E–3
Issuer key data, 6–3
Issuer PK Certificate, 6–3, 6–7, 8–7
Issuer Private Key, 6–11
Issuer Public Key, 1–9, 2–2, 6–9, 6–14
Issuer Public Key Certificate. *See* Issuer PK Certificate
Issuer Public Key data, 8–7
Issuer Public Key Exponent, 6–7, 8–7
Issuer Public Key Remainder, 6–7, 8–7
issuer script, 14–13, B–1, C–2, D–5
Issuer Script Command Counter, 11–4, 13–4, 13–10, 13–13, 14–7
issuer script commands, 14–8, C–1
Issuer Script Failure Indicator, 11–4, 11–10, 13–4, 13–10, 13–13, 14–7
Issuer Script Identifier, 14–8
Issuer Script Processed on Last Online Transaction, 11–10
Issuer Script Results, 14–8
Issuer Script Template, 14–8
issuer scripts. *See* Issuer-to-Card Script processing
Issuer-to-Card Script Processing, 2–5, 2–9, 8–15, 11–10, 12–9
  Authorization Response Data, 14–8
  card data, 14–7
  commands, 14–9
  processing flow, 14–13, 14–16
  terminal data, 14–8

K

keys, F–4 to F–5
Keys and Certificates for Offline Data Authentication, 6–3

L

Language Preference, 3–2, C–14
Last Online ATC Register, 9–2, 9–4 to 9–5, 11–10, 11–15, 13–4, 13–13, 13–15, C–7
List of AIDs Method, 1–7, 3–7, 3–10, 3–13
List of supported applications, 3–5
Lower Consecutive Offline Limit “9F14”, 9–2, 9–5
Lower Consecutive Offline Limit “9F58”, 11–4, 11–8, 11–10, 14–12, C–7, F–7

M

MAC, 14–7, 14–14, B–1 to B–2, C–2, C–8
MAC MDK, D–14
MAC Session Key, 14–14, B–2, B–8
MAC UDK, B–2, B–8
Magnetic Stripe Image, 15–3
mandatory, 1–3, A–44
Maximum Target Percentage to be used for Biased Random Selection, 9–3
MDK, D–13
Merchant Forced Transaction Online, 9–4
message integrity, 14–14, B–1 to B–2

N

new card, 9–4 to 9–5, 11–8, 11–15, 13–15, C–7, G–6

O

offline approval, 10–1, 11–16, 11–18, 13–7
offline CVM verification, C–18
Offline Data Authentication, 2–2, 2–8, 4–7, 5–3, 6–1, 6–7, 10–2
  DDA, 6–10
  Keys and Certificates, 6–3
  SDA, 6–7
offline decline, 10–1, 11–16, 13–7, G–6
Offline Decline Requested by Card Indicator, 11–4, 13–15, 13–17
Offline Enciphered PIN, 1–8, 6–5, 8–1, 8–7 to 8–8, 8–10 to 8–11, C–4
Offline PIN, 8–6, 11–15, 13–16
Offline PIN processing
  card data, 8–6
Offline PIN Verification not Performed (PIN Try Limit Exceeded), 11–8, 11–15, 13–16
Offline Plaintext PIN, 8–1, 8–8, 8–11
online authorization, 10–1, 11–8, 11–16, 11–18, 13–7, 13–9
Online Authorization Indicator, 1–8 to 1–9, 11–4, 11–9, 11–18, 13–4, 13–10, 13–13
Online Authorization Not Completed (on previous transaction), 11–7, 11–9, G–6
Online Card Authentication, 2–5, 12–1
Online Card Authentication. *See* CAM
online PIN, 8–1
Online Processing, 2–5, 2–9, 4–7, 6–16 to 6–17, 8–15, 11–26 to 12–1, 13–1, 13–25, 14–17, G–6
  card data, 12–2
  flow, 12–8
  online response data, 12–4
  Processing, 12–5
  terminal data, 12–4
Online Processing Requested, Online Authorization Not Completed, 13–14
online request, 12–2, 12–5
Online Requested by Card Indicator, 11–5, 11–9 to 11–10, 11–12
online response, 12–5
Online Response Data, Online Processing, 12–4
optional, 1–3, A–44

P

PAN, 6–8, 9–2, 9–4, D–11
PAN Sequence Number, D–11
partial selection, 1–7, 3–10
Payment Systems Directory, 3–4, 3–8
Payment Systems Environment, 3–4, 3–6 to 3–7, 14–10
PDOL, 3–2, 3–4, 3–6, 4–1, 4–3, C–15, G–2, G–5
Personalization, D–14
personalization, 15–1, C–1, F–6
  Flexible Approach with VSDC, 15–3
  templates, 15–2
PIN, F–4 to F–5
PIN CHANGE/UNBLOCK command, 2–10, 8–6, 14–11, 14–15, C–1, C–8, F–7
PIN encipherment, 8–10
PIN pad, 8–9
PIN Try Counter, 8–6, 8–8 to 8–9, 8–11, 8–14, 11–5, 11–15, 14–11, C–7, F–7, G–5
PIN Try Limit, 8–6, 8–8, 8–11, 8–14, 11–8, 11–15, 11–17, 13–16, 14–11
PIN, changing, 14–11, C–9
PIN, unblocking, 14–11, C–9
PINs, cardholder-selected, 14–15
PIX, 3–2, 3–5
Plus, 3–2 to 3–3
post-issuance updates, 11–8, 12–1, F–4
processing overview, 2–1
Processing Restrictions, 2–3, 2–8, 7–1
  Application Effective Date, 7–5
  Application Expiration Date, 7–6
  Application Usage Control, 7–4
  Application Version Number, 7–3
  card data, 7–2
  processing, 7–3
  terminal data, 7–3
PUT DATA command, 2–10, 14–12, C–1, C–11, F–7, G–7
PVV, 14–12, 14–15

R

Random Transaction Selection, 9–4
Read Application Data, 2–2, 2–8, 4–7, 5–1, 6–16, 7–6, 8–14, 9–5, 10–5, 11–26
  processing, 5–3
  terminal data, 5–3
READ RECORD command, 2–10, 3–6 to 3–7, 5–2 to 5–3, C–1, C–14, F–4, F–7
Receive GENERATE AC Command, completion of, 13–9
recommended, 1–3
Reference PIN, 8–6, 8–9, 8–11, 14–11, C–8, D–14, F–7
reference PIN, B–3
referrals, 13–9, 13–11
required, 1–3, A–44
retrieval capability, data element, A–45

RID, 3–2, 3–5, 6–7, 6–9, 6–14, 8–7
RSA, 6–3

S

SDA, 2–2, 2–8, 5–1, 6–1, 6–7, 11–2, 11–7, 11–10
SDA failed on last transaction, 11–7, 11–10
SDA Failure Indicator, 6–9, 11–5, 11–10, 11–17, 13–10, 13–13, 13–17
SDA or DDA, determining which to perform Offline Data Authentication, 6–6
SDA Tag List, 1–7 to 1–8, 6–8, 6–10
Secondary Application Currency Code, 11–4 to 11–5, 11–13, 11–18, 13–3 to 13–4, 13–19, C–7
secret data, A–45
secure messaging, 14–7, 14–13, B–1, C–2
Security Domain, F–2 to F–3
SELECT command, 2–10, 3–6, 3–11, 14–10, C–1, C–14, F–2
Session Key Generation, 1–9, B–8
Short File Identifier, 3–4, 3–6, 5–2, 14–12, 14–15, C–14, F–4
signature, cardholder, 8–1
Signed Dynamic Application Data, 6–12 to 6–13, 6–15, 11–19
Signed Static Application Data, 6–8, 6–10, 10–2, D–14, G–3
skimming, 6–1
special device, 14–10, A–45
Standard DDA, 2–2, 2–8, 6–10, 6–13, 6–15
Static Data Authentication Failure Indicator, 13–4
Static Data Authentication Failure Indicator. *See* SDA Failure Indicator
static data elements, A–45
stolen cards, 8–1, 14–11
Subsequent Related Processing, 14–17
  Application Selection, 3–14
  Cardholder Verification, 8–14
  Completion, 13–25
  Read Application Data, 5–3
  Terminal Action Analysis, 10–5
  Terminal Risk Management, 9–6

T

TACs, 10–3 to 10–4
Target Percentage to be used for Random Selection, 9–3
TC, 11–2, 11–16, 11–18 to 11–19, 13–5, 13–9, 13–11 to 13–12, 13–17, C–4, D–1, D–4, D–10, E–1
TC Hash Value, 10–3 to 10–4, D–2
TDOL, 10–3, D–2
Terminal Action Analysis, 2–4, 2–9, 6–17, 7–6, 8–14, 9–6 to 10–1, 11–26
  card data, 10–2
  processing, 10–4
  terminal data, 10–3
Terminal Country Code, 4–3 to 4–4, 7–3, 11–2 to 11–3, 11–5, 11–11, 11–17 to 11–18, 13–6, 13–18, D–3, E–2
terminal data
  for Application Selection, 3–5
  for Card Action Analysis, 11–5
  for Cardholder Verification, 8–8
  for DDA, 6–13
  for Issuer-to-Card Script Processing, 14–8
  for Processing Restrictions, 7–3
  for Read Application Data, 5–3
  for Terminal Action Analysis, 10–3
  for Terminal Risk Management, 9–3
terminal floor limit, 9–3
Terminal Floor Limit. *See also* floor limit checking
Terminal Risk Management, 2–3, 2–9, 9–1, 15–3
  card data, 9–2
  processing, 9–4
  terminal data, 9–3
terminal velocity checking, 9–4
terminated transactions, 1–3
Threshold Value for Biased Random Selection, 9–3
Track 1 Discretionary Data, 14–15
Track 2 Equivalent Data, 14–15
transaction authorized online, Completion, 13–9
Transaction Currency Code, 11–2, 11–5, 11–11 to 11–12, 11–17 to 11–18, 13–6, 13–18, D–3, E–2, G–2, G–4 to G–5
Transaction Date, 7–3, 7–6, D–3, E–2
transaction flow, sample, 2–7
Transaction Log, 9–3
Transaction PIN, 8–6, 8–8 to 8–9, 8–11
Transaction Status Information (TSI), 9–3, 14–8
Transaction Type, 7–3, D–3, E–2, G–5
TVR, 7–4 to 7–5, 9–3, 10–2, 11–2, 11–5, 11–17, 13–6, 13–17, 14–8, D–3, E–2

U

UDKs, 12–3, 12–6, D–11, D–13 to D–14
unable to go online, 13–9, 13–14, 13–17
Unpredictable Number, 6–11, 6–13, D–3, E–2
update capability, data element, A–45
UPDATE RECORD command, 2–10, 14–12, 14–15, C–1, C–16, F–4, F–7
Upper Consecutive Offline Limit, 13–4

Upper Consecutive Offline Limit “9F23”, 9–2, 9–5
Upper Consecutive Offline Limit “9F59”, 13–15, 14–12, C–7, C–12, F–7

V

velocity checking, 11–1, 13–15 to 13–16, G–6
velocity checking, terminal, 9–5, C–7
VERIFY command, 2–10, 8–6, 8–8, 8–11, 11–15, C–1, C–18, F–3
Visa, 3–2 to 3–3, G–5
Visa Certificate Authority, 6–3
Visa Certificate Authority User's Guide, 6–4
Visa discretionary data, C–4
Visa documentation, 1–11
Visa Electron, 3–2 to 3–3, G–5
Visa Integrated Circuit Card Specification, 1–1 to 1–2
  impact summary, 1–7
  revisions, 1–7
Visa Low-value Payment, 1–8 to 1–9, 4–4, G–1
Visa Private Key, 6–3, 8–7
Visa Public Key, 6–3, 6–9, 8–7
VisaNet, E–3
VLP
  duplicate data elements, G–3
  reset transaction, G–7
  transaction flow, G–8
  updating VLP limits, G–7
VLP Available Funds, G–1 to G–2, G–5, G–7
VLP Funds Limit, 14–12, C–7, C–12, F–7, G–1 to G–2, G–7
VLP Issuer Authorization Code, G–2, G–6
VLP Single Transaction Limit, 14–12, C–7, C–12, F–7, G–1 to G–2, G–5, G–7
VLP Terminal Support Indicator, G–2, G–4 to G–5
VLP Terminal Transaction Limit, G–1, G–4 to G–5
VSDC Flexible Approach Personalization Considerations, 15–3

Y

Y1 Authorization Response Code, 13–6
Y3 Authorization Response Code, 13–6, 13–9, 13–14, 13–17

Z

Z1 Authorization Response Code, 13–6
Z3 Authorization Response Code, 13–6, 13–9, 13–14, 13–17