Visa Integrated Circuit Card Specification (VIS)

Version 1.6

January 2016

Visa Confidential

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

THIS SPECIFICATION IS PROVIDED ON AN “AS IS”, “WHERE IS”, BASIS, “WITH ALL FAULTS” KNOWN AND UNKNOWN. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE LICENSED WORK AND TITLES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

THE INFORMATION CONTAINED HEREIN IS PROPRIETARY AND CONFIDENTIAL AND MUST BE MAINTAINED IN CONFIDENCE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE WRITTEN AGREEMENT BETWEEN YOU AND VISA INC., VISA INTERNATIONAL SERVICE ASSOCIATION, AND/OR VISA EUROPE LIMITED.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Contents

Chapter 1 • About This Specification

1.1 Audience . . . 21
1.2 VIS Update . . . 22
1.3 Terminology . . . 22
1.3.1 Mandatory/Required/Recommended/Optional . . . 22
1.3.2 Implement/Enable/Support . . . 22
1.3.3 Card/Application/Integrated Circuit . . . 23
1.3.4 Terminated Transactions . . . 23
1.3.5 Presence of Data Elements . . . 23
1.3.6 Notation . . . 23
1.3.7 Coding of RFU Values in Data Elements . . . 23
1.4 Document Structure . . . 24
1.4.1 Volume Overview . . . 24
1.4.2 Chapter Overview . . . 24
1.4.3 Subheading Overview . . . 26
1.4.4 Flowcharts . . . 27
1.5 Revisions to This Specification . . . 27
1.6 Impact Summary . . . 27
1.7 Reference Materials . . . 28
1.7.1 International Organisation for Standardisation (ISO) Documents . . . 29
1.7.2 Federal Information Processing Standards (FIPS) Publication . . . 29
1.7.3 EMV Documents . . . 30
1.7.4 Visa Documents . . . 30

Chapter 2 • Processing Overview

2.1 Functional Overview . . . 33
2.1.1 Application Selection (mandatory) . . . 33
2.1.2 Initiate Application Processing/Read Application Data (mandatory) . . . 33
2.1.3 Offline Data Authentication . . . 34
2.1.4 Processing Restrictions (mandatory) . . . 34
2.1.5 Cardholder Verification (mandatory) . . . 35
2.1.6 Terminal Risk Management (mandatory) . . . 35
2.1.7 Terminal Action Analysis (mandatory) . . . 35
2.1.8 Card Action Analysis (mandatory) . . . 36
2.1.9 Online Processing . . . 36

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2.1.10 Completion (mandatory) . . . 37
2.1.11 Issuer-to-Card Script Processing . . . 37
2.2 Mandatory and Optional Functionality . . . 39
2.2.1 Card Functional Requirements . . . 39
2.2.2 Command Support Requirements . . . 42

Chapter 3 • Application Selection

3.1 Card Data . . . 46
3.2 Terminal Data . . . 50
3.3 Commands . . . 51
3.4 Building the Candidate List . . . 52
3.4.1 Directory Selection Method . . . 52
3.4.2 List of AIDs Method . . . 54
3.5 Identifying and Selecting the Application . . . 56
3.6 Flow . . . 57
3.7 Subsequent Related Processing . . . 59

Chapter 4 • Initiate Application Processing

4.1 Card Data . . . 62
4.2 Terminal Data . . . 64
4.3 GET PROCESSING OPTIONS Command . . . 65
4.4 Processing . . . 65
4.5 Profiles Functionality . . . 66
4.5.1 Profile Selection . . . 67
4.5.2 Profile Behavior for Initiate Application Processing . . . 68
4.6 Prior Related Processing . . . 70
4.7 Subsequent Related Processing . . . 70

Chapter 5 • Read Application Data

5.1 Card Data . . . 74
5.2 Terminal Data . . . 75
5.3 READ RECORD Command . . . 75
5.4 Processing . . . 75
5.5 Prior Related Processing . . . 75
5.6 Subsequent Related Processing . . . 75

Chapter 6 • Offline Data Authentication

6.1 Keys and Certificates . . . 78
6.1.1 Visa Certificate Authority (CA) . . . 78
6.1.2 RSA Key Pairs . . . 78
6.1.2.1 Visa Public/Private Keys . . . 78

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.1.2.2 Issuer Public/Private Keys . . . 79
6.1.2.3 ICC Public/Private Keys . . . 80
6.2 Card Data . . . 80
6.3 Terminal Data . . . 85
6.4 Determining Whether to Perform SDA, DDA, or CDA . . . 86
6.5 Static Data Authentication (SDA) . . . 87
6.5.1 Processing . . . 87
6.6 Dynamic Data Authentication (DDA and CDA) . . . 88
6.6.1 Commands . . . 88
6.6.1.1 INTERNAL AUTHENTICATE Command . . . 88
6.6.1.2 GENERATE APPLICATION CRYPTOGRAM (AC) Command . . . 89
6.6.2 Processing . . . 89
6.6.2.1 DDA . . . 89
6.6.2.2 CDA . . . 91
6.7 Prior Related Processing . . . 91
6.8 Subsequent Related Processing . . . 92

Chapter 7 • Processing Restrictions

7.1 Card Data . . . 94
7.2 Terminal Data . . . 95
7.3 Processing . . . 95
7.3.1 Application Version Number . . . 95
7.3.2 Application Usage Control . . . 96
7.3.3 Application Effective Date . . . 97
7.3.4 Application Expiration Date . . . 98
7.4 Prior Related Processing . . . 98
7.5 Subsequent Related Processing . . . 98

Chapter 8 • Cardholder Verification

8.1 Card Data . . . 100
8.2 Terminal Data . . . 104
8.3 Commands . . . 105
8.4 Processing . . . 106
8.4.1 CVM List Processing . . . 106
8.4.2 Offline PIN Processing . . . 108
8.4.3 Processing of Other CVMs . . . 113
8.5 Prior Related Processing . . . 113
8.6 Subsequent Related Processing . . . 113

Chapter 9 • Terminal Risk Management

9.1 Card Data . . . 116

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

9.2 Terminal Data . . . 117
9.3 GET DATA Command . . . 118
9.4 Processing . . . 118
9.4.1 Terminal Exception File . . . 118
9.4.2 Merchant Forced Transaction Online . . . 118
9.4.3 Floor Limits . . . 118
9.4.4 Random Transaction Selection . . . 118
9.4.5 Terminal Velocity Checking . . . 119
9.4.6 New Card Check . . . 119
9.5 Prior Related Processing . . . 119
9.6 Subsequent Related Processing . . . 120

Chapter 10 • Terminal Action Analysis

10.1 Card Data . . . 122
10.2 Terminal Data . . . 124
10.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command . . . 124
10.4 Processing . . . 125
10.4.1 Review Offline Processing Results . . . 125
10.4.1.1 IAC Usage Example . . . 125
10.4.1.2 Terminal IAC and TAC Processing Steps . . . 126
10.4.2 Request Cryptogram Processing . . . 127
10.5 Prior Related Processing . . . 127
10.6 Subsequent Related Processing . . . 127

Chapter 11 • Card Action Analysis

11.1 Card Data . . . 130
11.2 Terminal Data . . . 138
11.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command . . . 139
11.4 Processing . . . 139
11.4.1 Card Receives Cryptogram Request . . . 139
11.4.2 Card Risk Management Overview . . . 140
11.4.3 Card Risk Management Checks . . . 143
11.4.3.1 Online Authorization Not Completed . . . 143
11.4.3.2 Issuer Authentication Failed (or Mandatory and Not Performed) on Last Transaction . . . 144
11.4.3.3 Static Data Authentication (SDA) Failed on Last Transaction . . . 144
11.4.3.4 Offline Dynamic Data Authentication (DDA or CDA) Failed on Last Transaction . . . 144
11.4.3.5 Issuer Script Processed on Last Online Transaction . . . 145
11.4.3.6 Velocity Checking for Consecutive Transactions Lower Limit . . . 145

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.7 Velocity Checking for Consecutive International Transactions Lower Limit . . . 147
11.4.3.8 Velocity Checking for Consecutive International Country Transactions Lower Limit . . . 149
11.4.3.9 Velocity Checking for Cumulative Total Transaction Amount Lower Limit . . . 150
11.4.3.10 Velocity Checking for Contactless Offline Transactions Lower Limit . . . 154
11.4.3.11 Velocity Checking for VLP Contactless Transactions Reset Threshold . . . 154
11.4.3.12 New Card . . . 155
11.4.3.13 Offline PIN Verification Not Performed (PIN Try Limit Exceeded) . . . 156
11.4.3.14 Go Online on Next Transaction From Previous Online Response . . . 156
11.4.3.15 Special Transactions . . . 157
11.4.3.16 PIN Verification Not Performed or Not Successful for a PIN-Expecting Card . . . 157
11.4.3.17 VERIFY Not Received by PIN-Expecting Card . . . 157
11.5 Card Provides Response Cryptogram . . . 158
11.5.1 Card Declined Transaction Offline . . . 159
11.5.2 Card Requested Online Processing . . . 162
11.5.3 Card Approved Transaction Offline . . . 162
11.5.4 CDA Requested . . . 165
11.6 Processing Flow . . . 166
11.7 Prior Related Processing . . . 168
11.8 Subsequent Related Processing . . . 168

Chapter 12 • Online Processing

12.1 Card Data . . . 170
12.2 Online Response Data . . . 172
12.3 EXTERNAL AUTHENTICATE Command . . . 173
12.4 Processing . . . 173
12.4.1 Online Request . . . 174
12.4.2 Online Response . . . 174
12.4.3 Issuer Authentication using the EXTERNAL AUTHENTICATE command . . . 175
12.5 Processing Flow . . . 177
12.6 Prior Related Processing . . . 178
12.7 Subsequent Related Processing . . . 178

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Chapter 13 • Completion Processing

13.1 Card Data . . . 180
13.2 Terminal Data . . . 188
13.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command . . . 190
13.4 Completion Processing Overview and Flow . . . 190
13.5 Receive GENERATE AC Command . . . 192
13.6 Processing Response Data for Online Authorized Transaction . . . 192
13.6.1 Issuer Authentication During Second GENERATE AC for CVN 10 . . . 193
13.6.2 Issuer Authentication for CVN 18 and CVN '22' . . . 194
13.6.2.1 Card Updates Processing Using the Verified CSU . . . 195
13.6.2.2 Counter Updates Processing Using the Verified CSU . . . 196
13.7 Complete Response for Online Authorized Transaction . . . 202
13.7.1 Decline Requested After Online Authorization . . . 203
13.7.2 Approval Requested After Online Authorization . . . 206
13.7.2.1 Card Approves Transaction After Approval Requested . . . 208
13.7.2.2 Card Declines Transaction After Approval Requested . . . 213
13.8 Online Processing Requested, Online Authorization Not Completed . . . 215
13.8.1 Card Risk Management . . . 215
13.8.1.1 Velocity Checking for Consecutive Transactions Upper Limit . . . 216
13.8.1.2 New Card . . . 217
13.8.1.3 PIN Try Limit Exceeded . . . 217
13.8.1.4 Velocity Checking for Cumulative Total Transaction Amount Upper Limit . . . 218
13.8.1.5 Velocity Checking for Consecutive International Transactions Upper Limit . . . 219
13.8.1.6 Velocity Checking for Consecutive International Country Transactions Upper Limit . . . 221
13.8.1.7 PIN Verification Not Performed or Failed for a PIN-Expecting Card . . . 222
13.8.2 Card Response After Unable to Go Online . . . 223
13.8.2.1 Card Declines (AAC) Transaction After Unable to Go Online . . . 223
13.8.2.2 Card Approves (TC) Transaction After Unable to Go Online . . . 225
13.9 CDA Requested . . . 228
13.10 Prior Related Processing . . . 229
13.11 Subsequent Related Processing . . . 229

Chapter 14 • Issuer-to-Card Script Processing

14.1 Key Management for Issuer Script Processing . . . 232
14.2 Card Data . . . 237
14.3 Terminal Data . . . 239

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14.4 Authorization Response Data . . . 240
14.5 Commands . . . 241
14.5.1 APPLICATION BLOCK . . . 241
14.5.2 APPLICATION UNBLOCK . . . 242
14.5.3 CARD BLOCK . . . 242
14.5.4 PIN CHANGE/UNBLOCK . . . 243
14.5.5 PUT DATA . . . 243
14.5.6 UPDATE RECORD . . . 243
14.6 Processing . . . 244
14.6.1 Authorization Response Message . . . 244
14.6.2 Card Script Processing . . . 244
14.6.3 Card Secure Messaging . . . 245
14.6.4 Other Considerations . . . 246
14.6.5 Resulting Indicators for Script Processing . . . 246
14.6.6 Processing Flow . . . 248
14.7 Prior Related Processing . . . 249
14.8 Subsequent Related Processing . . . 249

Appendix A • VIS Data Element Tables

A.1 Data Element Descriptions . . . 252
A.1.1 Name, Format, Template/Tag, Length and Source . . . 252
A.1.2 Requirement . . . 253
A.1.3 Update Capability, Update, Retrieval, Backup, Secret . . . 253
A.1.3.1 Update Capability (UC) . . . 253
A.1.3.2 Issuer Update . . . 255
A.1.3.3 Retrieval . . . 255
A.1.3.4 Backup . . . 256
A.1.3.5 Secret Data . . . 257
A.2 Data Element Tags . . . 407

Appendix B • Secure Messaging

B.1 Secure Messaging Format . . . 418
B.2 Message Integrity and Authentication (MACing) . . . 418
B.2.1 MAC Placement . . . 418
B.2.2 MAC Length . . . 418
B.2.3 MAC Key Generation . . . 418
B.2.4 MAC Computation . . . 418
B.3 Data Confidentiality . . . 421
B.3.1 Data Encipherment Key Calculation . . . 421
B.3.2 Enciphered Data Structure . . . 421

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

B.3.3 Data Encipherment Calculation . . . 421
B.3.4 Data Decipherment Calculation . . . 423
B.4 Secure Messaging Session Key Generation . . . 424
B.4.1 XOR Session Key Generation . . . 424
B.4.2 EMV Common Session Key Generation . . . 424
B.5 Secure Messaging Impact on Command Formats . . . 426

Appendix C • Commands for Financial Transactions

C.1 Basic Processing Rules for Issuer Script Commands . . . 430
C.2 APPLICATION BLOCK Command—Response Application Protocol Data Units (APDUs) 431
C.2.1 Processing State Returned in the Response Message . . . 431
C.3 APPLICATION UNBLOCK Command—Response APDUs . . . 432
C.3.1 Processing State Returned in the Response Message . . . 432
C.4 CARD BLOCK Command—Response APDUs . . . 433
C.4.1 Processing State Returned in the Response Message . . . 433
C.5 EXTERNAL AUTHENTICATE Command—Response APDUs . . . 434
C.5.1 Processing State Returned in the Response Message . . . 434
C.6 GENERATE APPLICATION CRYPTOGRAM (AC) Command—Response APDUs 435
C.6.1 Processing State Returned in the Response Message . . . 435
C.7 GET CHALLENGE Command—Response APDUs . . . 437
C.7.1 Processing State Returned in the Response Message . . . 437
C.8 GET DATA Command—Response APDUs . . . 438
C.8.1 Command Support . . . 438
C.8.2 Data Retrievable by GET DATA Command . . . 438
C.8.2.1 Special Devices . . . 438
C.8.2.2 Financial Transactions . . . 439
C.8.3 Processing State Returned in the Response Message . . . 439
C.9 GET PROCESSING OPTIONS Command—Response APDUs . . . 440
C.9.1 Processing State Returned in the Response Message . . . 440
C.10 INTERNAL AUTHENTICATE Command—Response APDUs . . . 442
C.10.1 Processing State Returned in the Response Message . . . 442
C.11 PIN CHANGE/UNBLOCK Command—Response APDUs . . . 443
C.11.1 PIN Data Generated Using the Current PIN . . . 443
C.11.2 PIN Data Generated Without Using the Current PIN . . . 446
C.11.2.1 VIS Legacy PIN Block Format Generated Without Using the Current PIN . . . 446
C.11.2.2 ISO PIN Block Format Generated Without Using the Current PIN . . . 448
C.11.3 Processing State Returned in the Response Message . . . 449

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.12 PUT DATA Command—Response APDUs . . . 451
C.12.1 Command Message . . . 451
C.12.2 Reset Offline Funds with Update to Funds Limits . . . 454
C.12.3 Update AIP and AFL . . . 454
C.12.4 Processing State Returned in the Response Message . . . 454
C.13 READ RECORD Command—Response APDUs . . . 456
C.13.1 Processing the Profile Selection File Entries . . . 456
C.13.2 Processing State Returned in the Response Message . . . 456
C.14 SELECT Command—Response APDUs . . . 457
C.15 UPDATE RECORD Command—Response APDUs . . . 458
C.15.1 Command Message . . . 458
C.15.2 Processing State Returned in the Response Message . . . 459
C.16 VERIFY Command—Response APDUs . . . 461
C.16.1 Processing State Returned in the Response Message . . . 461

Appendix D • Authentication Data, Keys and Algorithms

D.1 Source Data for Application Cryptograms (TC, AAC, ARQC) . . . 464
D.2 Application Cryptograms . . . 466
D.2.1 Cryptogram Version Numbers (CVNs) Supported . . . 466
D.2.2 Application Cryptogram Algorithm . . . 466
D.3 CVN 10 (Cryptogram Version Number = '0A') . . . 468
D.3.1 Data Input for CVN 10 ('0A') . . . 468
D.3.2 Generating the Application Cryptogram (TC, AAC, and ARQC) for CVN 10 ('0A') . . . 470
D.3.3 Generating the Authorization Response Cryptogram (ARPC) for CVN 10 ('0A') . . . 471
D.3.4 Format of Issuer Authentication Data (IAuD) for CVN 10 ('0A') . . . 472
D.4 CVN 18 (Cryptogram Version Number '12') and CVN '22' . . . 473
D.4.1 Data Input for CVN 18 ('12') and CVN '22' . . . 473
D.4.2 Generating the Application Cryptogram (TC/AAC/ARQC) for CVN 18 ('12') and CVN '22' . . . 475
D.4.3 Generating the Authorization Response Cryptogram (ARPC) for CVN 18 ('12') and CVN '22' . . . 476
D.4.4 Format of Issuer Authentication Data (IAuD) for CVN 18 ('12') and CVN '22' 476
D.5 CVN 12 ('0C'), CVN '2C', and CVN 50 ('32') - CVN 59 ('3B') . . . 477
D.6 Data Conversion . . . 478
D.6.1 All Data . . . 478
D.6.2 Numeric Data . . . 478
D.6.3 Compressed Numeric Data . . . 479
D.6.4 Binary Data . . . 479

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.6.5 Alphanumeric and Alphanumeric Special Data . . . 479
D.7 Derivation Key Methodology . . . 480
D.7.1 Unique DEA Keys Derivation . . . 480
D.7.2 EMV Common Session Key Derivation . . . 483
D.8 Host Security Modules (HSM) . . . 484
D.8.1 Real-Time Host-Based Cryptographic Functions . . . 484
D.8.2 Personalization Support Cryptographic Functions . . . 485

Appendix E • Profiles Functionality

E.1 Profile Selection . . . 488
E.1.1 Building Profile Selection Input Data . . . 489
E.1.2 Profile Selection Entries . . . 489
E.1.3 Profile Selection File Processing . . . 495
E.1.4 Profile Selection Example . . . 499
E.2 Profile Behavior . . . 502
E.2.1 Using the Profile Control . . . 504
E.2.2 Default Application Behavior for Profiles Functionality . . . 507
E.3 Minumum Support for Profiles Functionality . . . 508

Appendix F • Issuer Application Data and Card Verification Results Formats

F.1 Issuer Application Data (IAD) Formats . . . 510
F.2 Card Verification Results (CVR) Format for IAD Formats . . . 512
F.3 Determining the IAD Format . . . 514

Appendix G • Overview of Velocity-Checking Counters

G.1 Counter Overflow . . . 517

Appendix H • Dual-Interface Contactless and Contact

H.1 Common Data . . . 520
H.2 Data Accessibility . . . 520
H.2.1 Record Data Restricted by Interface . . . 520
H.2.2 Transaction Log Records Restricted by Interface . . . 520
H.2.3 Application Internal Data Elements . . . 521
H.3 New Functionality by Section . . . 522
H.3.1 Initiate Application Processing (Chapter 4) . . . 522
H.3.2 First GENERATE AC Command Verification (Chapter 11) . . . 522
H.3.3 Second GENERATE AC Command Verification (Chapter 13) . . . 522
H.3.4 Issuer-to-Card Script Processing (Chapter 14) . . . 523
H.3.5 Data Dictionary (Appendix A) . . . 523
H.3.6 Commands for Financial Transactions (Appendix C) . . . 523
H.3.7 Issuer Discretionary Data Options (Appendix J) . . . 524

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Appendix I • Transaction Log

Appendix J • Issuer Discretionary Data Options

J.1 Issuer Discretionary Data Options . . . 528
J.2 Personalization for IDD . . . 531
J.3 Issuer Application Data Returned in GENERATE AC . . . 532
J.4 MAC Calculation . . . 533
J.4.1 Padding for IDD MAC Generation . . . 534
J.5 Issuer Discretionary Data Example . . . 535

Glossary . . . 537

Index . . . 563

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Tables

2-1: Card Functional Requirements . . . 39
2-2: Command Support Requirements . . . 42
3-1: Application Selection—Card Data . . . 46
3-2: Application Selection—Terminal Data . . . 50
3-3: Sample Matching AIDs . . . 54
4-1: Initiate Application Processing—Card Data . . . 62
4-2: Initiate Application Processing—Terminal Data . . . 64
5-1: Read Application Data—Card Data . . . 74
6-1: Offline Data Authentication—SDA, DDA and CDA Card Data . . . 80
6-2: Offline Data Authentication—DDA and CDA Terminal Data . . . 85
7-1: Processing Restrictions—Card Data . . . 94
7-2: Processing Restrictions—Terminal Data . . . 95
7-3: Application Usage Control (AUC) . . . 97
8-1: CVM List Processing—Card Data . . . 100
8-2: PIN Processing—Terminal Data . . . 104
8-3: Sample CVM List . . . 107
9-1: Terminal Risk Management—Card Data . . . 116
9-2: Terminal Risk Management—Terminal Data . . . 117
10-1: Terminal Action Analysis—Card Data . . . 122
10-2: Terminal Action Analysis—Terminal Data . . . 124
11-1: Card Action Analysis—Card Data . . . 130
11-2: Card Action Analysis—Terminal Data . . . 138
11-3: Card Risk Management Checks . . . 140
11-4: Card's Response to First GENERATE AC Command . . . 158
12-1: Online Processing, Issuer Authentication—Card Data . . . 170
12-2: Online Processing, Issuer Authentication—Terminal Data . . . 172
13-1: Completion—Card Data . . . 180
13-2: Completion—Terminal Data . . . 188
14-1: Issuer-to-Card Script Processing—Card Data . . . 237

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14-2: Issuer-to-Card Script Processing—Terminal Data 239
14-3: Issuer-to-Card Script Processing—Online Response Data 240
A-1: Data Element Descriptions 258
A-2: Data Element Tags 407
C-1: GENERATE AC Command Validation Error Responses 436
C-2: GET DATA Response Data Field for Constructed Data Object 439
C-3: GET DATA Command Validation Error Responses 439
C-4: Data Retrieval Using GET PROCESSING OPTIONS 440
C-5: GET PROCESSING OPTIONS Command Validation Error Responses . . 440
C-6: INTERNAL AUTHENTICATE Command Validation Error Responses . . . 442
C-7: PIN CHANGE/UNBLOCK Command Validation Error Responses 450
C-8: PUT DATA Command Message 452
C-9: PUT DATA Command Data for P1 P2 = Primitive Data Element Tag . . . 453
C-10: PUT DATA Command Data for P1 P2 = '0000' or Template Tag 453
C-11: PUT DATA Command Validation Error Responses 454
C-12: PUT DATA Command Message Error Conditions 455
C-13: READ RECORD Command Validation Error Responses 456
C-14: UPDATE RECORD Command Message 458
C-15: UPDATE RECORD Reference Control Parameter 459
C-16: UPDATE RECORD Command Validation Error Conditions 459
C-17: UPDATE RECORD Response Additional Error and Warning Conditions . . 460
C-18: VERIFY Command Validation Error Responses 461
D-1: Data Input for TC, AAC and ARQC With CVN 10 469
D-2: Data Input for TC, AAC, ARQC With CVN 18 474
E-1: Data Elements in Profile Selection Entry 491
E-2: Profile Selection Example – Profiles 499
E-3: Profile Selection Example – Profile Selection File 500
E-4: Profile Selection Example – PDOL Contents 500
E-5: Profile Selection Entries – Complex Example 501
F-1: IAD Formats 510

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

F-2: Card Verification Results (CVR) Formats for IAD Format 0/1/3 and IAD Format 2 512

G-1: Velocity-checking Counters Used in VIS 516

J-1: IDD Options 529

J-2: MAC Calculation 533

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figures

2-1: Sample Transaction Flow 38
3-1: Sample Card Directory Structure 53
3-2: Application Selection Using Directory Method 57
3-3: Application Selection Using List of AIDs 58
4-1: Initiate Application Processing Flow 69
8-1: Checking The PIN Try Counter 108
8-2: PIN Encipherment 109
8-3: Offline PIN Processing. 112
11-1: Card Action Analysis Processing Flow (1 of 2) 166
11-2: Card Action Analysis Processing Flow (2 of 2) 167
12-1: Online Processing Flow 177
13-1: Completion Processing Flow 191
14-1: Generation and Use of MAC Keys 234
14-2: Generation and Use of Data Encipherment Keys 236
14-3: Issuer-to-Card Script Processing Flow 248
B-1: MAC Algorithm for Double-Length DEA Key 420
B-2: Data Encipherment for Double-Length DEA Key 422
B-3: Data Decipherment for Double-Length DEA Key 423
C-1: Input Block based on UDK-A 444
C-2: Input Block based on New PIN 444
C-3: Generation of PIN **CHANGE** Command Data With Current PIN 445
C-4: Generation of PIN **CHANGE** Command Data Without Current PIN 447
C-5: ISO PIN Block Format 1 448
C-6: ISO PIN Block Format 2 449
D-1: Algorithm for Generating the Application Cryptogram (TC, AAC or ARQC) . 467
D-2: Algorithm for Generating the ARPC for CVN 10 472
D-3: Derivation Method of Unique DEA Keys A and B 480
D-4: Using the Unique DEA Keys to Perform Card Authentication 482

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E-1: Profile Selection Input Data 489
E-2: Profile Selection Entry Format 490
E-3: Profile Selection Entry Processing Algorithm 498

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

1 About This Specification

The *Visa Integrated Circuit Card Specification* (VIS) provides the technical details of chip card functionality related to Visa Smart Debit/Credit (VSDC) transactions (Visa's chip-based credit and debit programs) over a contact chip interface. It focuses on the functions performed by the chip card 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 EMV™ specifications[1] to ease vendor development efforts (the EMV specifications are maintained by EMVCo, an organization of payment systems including Visa Inc., MasterCard Worldwide, JCB International and American Express).
- Aid customers 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 card applications used for contact chip-based credit and debit programs
- Identify options that customers and vendors can implement to meet market needs
- Support Visa's payment service rules and International Operating Regulations for Visa Smart Debit/Credit (VSDC)
- Define Visa's implementation of optional EMV features

VIS is based on, and complies with, all requirements in the EMV specifications and the mandatory EMV bulletins published on the EMVCo website (see section 1.7.3). The VIS and EMV specifications and any updates reflected in EMV bulletins or the VIS Updates List should be used together for reference and development purposes.

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 customers, vendors, and readers seeking a technical understanding of the functionality of chip cards and related functionality in terminals supporting Visa Smart Debit/Credit.

---

[1] EMV™ is a trademark owned by EMVCo LLC.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

1.2 VIS Update

This document serves as an update to VIS 1.4.1. The update includes changes reflecting updates to *EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.2*, enhancements to VIS functionality, and corrections and clarifications to VIS 1.4.1. An impacts summary highlighting the differences between VIS 1.4.1 and the current version, VIS 1.5, is provided later in this chapter.

1.3 Terminology

This section clarifies several terms and notation 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, shall not interfere with global interoperability.

Note: *The term "must" is used in descriptive text when the requirement is stated elsewhere (for example, in another specification) or is beyond the scope of the card or application.*

1.3.2 Implement/Enable/Support

When used to describe card or application functionality, the following terminology may be used:

"implemented" — functionality that the application is capable of performing. The phrase "implement support for" may also be used.

"enabled" — functionality that is activated or turned on (for example, by personalizing the relevant data).

"disabled" — functionality that has been deactivated or turned off (for example, by not personalizing the relevant data).

"supported" — functionality that is both implemented and enabled.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

1.3.3 Card/Application/Integrated Circuit

In general, the term “card” or “application” is used to describe functions performed by the VIS 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.

1.3.4 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.

1.3.5 Presence of Data Elements

In general, the term “present” is used to describe that a data element has either been personalized or has been added to the application post-issuance by a PUT DATA command. For counters, the term “present” is used if the functionality associated with that type of counter is implemented in the application.

If a card condition evaluates a data element that is not present, then the specific condition referencing the data element shall evaluate to FALSE, unless explicitly stated otherwise, for card requirements or statements with multiple conditions, all other conditions in the requirement or statement are unaffected and evaluated as normal.

If a card action is to be performed on a data element that is not present, then the specific action is not performed. For requirements where multiple actions are to be taken, all other actions in the set are unaffected and performed as normal.

1.3.6 Notation

0 to 9	10 decimal digits. Decimal numbers are not enclosed in quotation marks.
'0' to '9', 'A' to 'F'	16 hexadecimal characters. Hexadecimal characters are enclosed in single straight quotation marks.
xb, xxxb	Binary values. Bit values are appended with the character “b” (for example, 1b and 0010b). Bits within a byte are numbered from right to left, where the low-order bit (bit 1) is the rightmost bit and the high-order bit (bit 8) is the leftmost bit.
‘Bit Name’	The bit defined as “Bit Name” within a data element. Bit names are enclosed in single curly quotation marks.

1.3.7 Coding of RFU Values in Data Elements

Values in data elements marked as RFU (Reserved for Future Use) shall be set to zero, and the card shall not act on, operate on, or verify RFU data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Coding of data marked as RFU shall follow the same rules as defined in EMV Book 3, section 6.3.6.

1.4 Document Structure

This section provides an overview of the structure of the *Visa Integrated Circuit Card Specification*, followed by an overview of each chapter in this Specification, and concludes with the sub-heading structure of each chapter.

1.4.1 Volume Overview

VIS consists of this one volume and specifies the technical details of EMV related to the data and processing performed by the card, and provides information about all card, issuer, terminal, and acquirer data elements. It also includes additional Visa specific requirements for card functionality. Vendors involved in the creation of a VIS contact or dual-interface (VIS contact and VCPS contactless) chip card application should focus on this document for their development efforts.

Terminal functionality is defined by the EMV specification. Visa-specific requirements for terminals are described in the *Visa Transaction Acceptance Device Requirements*. Additional information about Visa-specific implementations for terminals is in the *Visa Transaction Acceptance Device Guide.* Contact your regional representative for more information about the *Visa Transaction Acceptance Device Guide* and *Visa Transaction Acceptance Device Requirements*.

To provide clarity, requirements and information from EMV, the *Visa Transaction Acceptance Device Guide* and *Visa Transaction Acceptance Device Requirements* may be restated in the VIS Card Specification to provide comprehensive information.

1.4.2 Chapter Overview

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

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

Chapter 2, Processing Overview—Provides an overview of functions and highlights whether each is mandatory or optional.

Chapter 3, Application Selection—This function determines which of the applications that are 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 that was requested by the card during Application Selection and configures the application to process the transaction.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 uses the issuer's host-based risk parameters to review and authorize or reject transactions sent online for authorization. The issuer host may send information in the response that can be used to authenticate that the online response came from the valid issuer, and to control updates to the card during completion.

Chapter 13, Completion Processing—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.

Appendix A, VIS Data Element Tables—Defines the data elements used in processing the VIS application.

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

Appendix C, Commands for Financial Transactions—Outlines the commands used during transaction processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Appendix D, Authentication Keys and Algorithms—Describes the keys, algorithms, and data elements associated with the generation of the online authentication cryptograms (ARQC, TC, AAC); and the associated authorization response cryptograms (ARPCs).

Appendix E, Profiles Functionality—Describes the optional Profiles Functionality that may be used to configure application data and the behavior used to customize transaction processing in different transaction environments.

Appendix F, Issuer Application Data and Card Verification Results Formats—Describes the two formats for Issuer Application Data (IAD) that may be used for transactions, and the associated Card Verification Results format associated with each IAD format.

Appendix G, Overview of Counters—Provides a simple summary of the types of counters used in this specification, indicates whether the counter tracks amounts or numbers of transactions, and identifies the lower and upper limit associated with each type of counter as well as whether the counter increments from zero or decrements from the maximum value.

Appendix H, Dual-Interface Contactless and Contact—Outlines additional processing in the contact chip application functionality for cards that support both contact chip functionality and contactless chip functionality such as qVSDC.

Appendix I, Transaction Log—Describes optional transaction log functionality.

Appendix J, Issuer Discretionary Data Options—Describes an option that permits issuers to more closely track funds at the host, by allowing placement of specific data into the Issuer Discretionary Data portion of the Issuer Application Data

Glossary—Defines acronyms and terminology used in this specification.

Index

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 implement the function.
- **Processing**—Provides the technical details of the function. If there are several functions within a process, they may be listed separately.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- **Processing Flow**—Provides a high-level flowchart illustrating the processing of a command.
- **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.

1.4.4 Flowcharts

Flowcharts provide a high-level overview of processing for a command.

Flowcharts are representative of processing and may not include all steps to be performed. Implementations are required to comply with the requirements in the text and are not required to strictly follow the flow diagrams. In the case of a discrepancy between a flowchart and the related text, the text shall take precedence.

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 Updates List or in an update to this document.

1.6 Impact Summary

Changes from the previous version, VIS 1.5 (May 2009) are listed in the VIS 1.5 Updates List 5 (which includes changes from prior versions of the VIS 1.5 Updates List).

The following lists major changes and additions in VIS 1.6:

- Addition of a new Issuer Application Data Format, IAD Format 2, and the corresponding addition of new Cryptogram Version Numbers (CVN) '22' and '2C') to be used with IAD Format 2.
- Addition of a requirement for applications to implement support for the cryptographic algorithm used for Cryptogram Version Number 18 and '22' (issuers may still choose to not use the algorithm).
- Addition of a new Secure messaging method (only available for IAD Format 2).
- Addition of a new card risk management for (offline) PIN-expecting cards
- Addition of new EMV data elements for tokenization and application selection, and new bit definitions in the Terminal Verification Results
- Addition of a card CDCVM indicator
- The Application Default Action is 6 bytes long, and additional bits are defined.
- Security enhancements and clarifications to VERIFY command processing

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Incorporation of detailed description of key derivation and Application Cryptogram algorithm used for Cryptogram Version Number 18 and '22'
- Clarification of functionality for online-only cards
- Clarifications to Issuer Authentication during EXTERNAL AUTHENTICATE versus second GENERATE AC
- Clarifications to the requirements restricting reading and updating of data by interface
- Clarification that SDA is no longer supported for contact chip transactions
- Clarification of requirements and recommendations for data to sign for dynamic offline data authentication
- Clarification of Authorization Response Code terminology
- Clarification of when Issuer Country Code must be present for card risk management checks to be performed
- Clarification to resetting of the PIN Try Counter using the Card Status Updates in the authorization response
- Clarifications to the values for Cardholder Name
- The Available Offline Spending Amount is no longer retrievable by the GET DATA command

Contact Visa Approval Services at approvalservices@visa.com for information on testing schedules.

1.7 Reference Materials

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

1.7.1 International Organisation for Standardisation (ISO) Documents

For information on ordering ISO documents, see http://www.iso.org.

- *ISO/FDIS 639-1. Codes for the Representation of Names and Languages (Alpha-2 code).*
- *ISO 3166. Codes for the Representation of Names of Countries.*
- *ISO 4217. Codes for the Representation of Currencies and Funds.*
- *ISO/IEC 7810. Identification Cards—Physical Characteristics.*
- *ISO/IEC 7811. Identification Cards—Recording Technique.*
- *ISO/IEC 7812. Identification Cards—Identification of Issuers.*
- *ISO/IEC 7813. Identification Cards—Financial Transaction Cards.*
- *ISO/IEC 7816-4. Identification Cards—Integrated Circuit Cards with Contacts—Part 4: Interindustry Commands for Interchange.*
- *ISO/IEC 7816-5. 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/IEC 8859. Information Processing—8-bit Single-Byte Coded Graphic Character Sets.*
- *ISO 9362. Banking—Banking telecommunication messages—Bank identifier codes.*
- *ISO 9564. Banking—Personal Identification Number Management and Security.*
- *ISO 13616. Banking and related financial services—International bank account number (IBAN).*

1.7.2 Federal Information Processing Standards (FIPS) Publication

Available on http://csrc.nist.gov

- *FIPS 46-3, Data Encryption Standard (DES).*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

1.7.3 EMV Documents

VIS application processing shall comply with current EMV requirements. If any mandatory changes to the EMV specification (excluding the Common Core Definitions part of the EMV specification) contradict this specification, VIS application processing shall be modified as needed to correspond to the mandatory EMV requirements, even if no update to this specification has been published.

The current version of the EMV specifications and bulletins are available on the EMVCo Website.

Available at: http://www.emvco.com/specifications.aspx

- *EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, November 2011.*
  - *Book 1, Application Independent ICC to Terminal Interface Requirements.*
  - *Book 2, Security and Key Management.*
  - *Book 3, Application Specification.*
  - *Book 4, Cardholder, Attendant and Acquirer Interface Requirements.*
- *EMV Card Personalization Specification (EMV-CPS), Version 1.1, July 2007.*

Available at: http://www.emvco.com/specifications.aspx

- Specification bulletins and other updates, including:
  - [EMV Tokenization] EMV Specification Bulletin 167, Payment Account Reference (PAR)
  - [EMV ASRPD] EMV Specification Bulletin 175, Application Selection Registered Proprietary Data.

1.7.4 Visa Documents

Contact your Visa representative for current versions of the following documents and other Visa reference documentation.

- VIS 1.5 Updates List
- *Visa Transaction Acceptance Device Guide*
- *Visa Transaction Acceptance Device Requirements*
- *Visa Contactless Payment Specification (VCPS), Version 2.2, January 2015.*
- *VSDC Personalization Specification for VIS and VCPS, Version 2.0*—A guide to personalization of VSDC Applications using the Common Personalization approach described in EMV-CPS.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- *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 VIS Issuers*—Describes best practices, suggestions, considerations, and step-by-step activities to assist with implementation for VSDC issuers of VIS cards.
- *VSDC System Technical Guide*—Describes changes to VisaNet to support VSDC cards.
- *Visa Security Guidelines - VSDC Applications*
- *Visa Security Guidelines - Multi-Application Platforms*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2 Processing Overview

This chapter provides an overview of a VIS 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.

This chapter includes the following sections:

2.1 Functional Overview

2.2 Mandatory and Optional Functionality

2.1 Functional Overview

The following functions are used in VIS 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, the terminal, or both.

2.1.1 Application Selection (mandatory)

When a VIS 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, then 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 VIS application is selected, then 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 or perform different internal processing 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2.1.3 Offline Data Authentication

The terminal determines whether it should authenticate the card offline using either 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 validates that the card data has not been fraudulently altered and that the card is genuine. Offline dynamic data authentication has two forms: Dynamic Data Authentication (DDA) and Combined DDA/AC Generation (CDA). In both forms, the terminal verifies the card static data in a similar manner to SDA.

With offline dynamic data authentication, the terminal requests that the card generate a cryptographic signature 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 CDA, the generation of the dynamic signature is combined with the generation of the card's Application Cryptogram during Card Action Analysis to ensure that the Application Cryptogram came from the valid card.

Note: *CDA is described in the EMV specifications. It is optional in VIS (as it is in EMV), and is not discussed in detail in this document. For more information, see the EMV specifications and bulletins.*

Note: *All chip cards that support offline authorization of contact chip transactions do not support SDA, do support DDA, and might optionally also support CDA. Throughout the remainder of this document, descriptions will continue to describe SDA so as to avoid confusion of the reader and to remain consistent with the functional descriptions in the underlying EMV specification.*

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 and services, or cashback.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, then 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 as the CVM.

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 the EMV specifications and bulletins. Terminal velocity checking results are considered during Terminal Action Analysis.

Visa recommends support for velocity checking be performed by the card using the card velocity checks in Card Action Analysis and the data elements used for card velocity checks defined by Visa instead of being performed by the terminal using the optional terminal velocity checks and EMV-defined data in Terminal Risk Management.

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 requested 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 CDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 and the card may convert a terminal request for an online transaction to 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 “proof” of a 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, then 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 and additional response data sent to the card, such as the ARPC Response Code or the Card Status Updates, and the card’s secret DES key). The response may also include post-issuance updates to the card either as part of the response data or as separate commands called Issuer Scripts.

Issuer Authentication is validation of the ARPC and the additional response data that would be used during completion. Validation of the ARPC verifies that the response came from the genuine issuer (or its agent). Issuer Authentication may be performed as part of either Online Processing or as part of Completion Processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If the authorization response contains an ARPC and the card supports Issuer Authentication, then the card performs Issuer Authentication (either during Online Processing, or as part of Completion Processing) by validating the ARPC. 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, then 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 Completion (mandatory)

The card and terminal perform final processing to complete the transaction.

If Issuer Authentication is supported but was not performed during Online Processing, then it may be performed during Completion, and the card may perform updates that were specified by the issuer in the data validated using Issuer Authentication.

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.

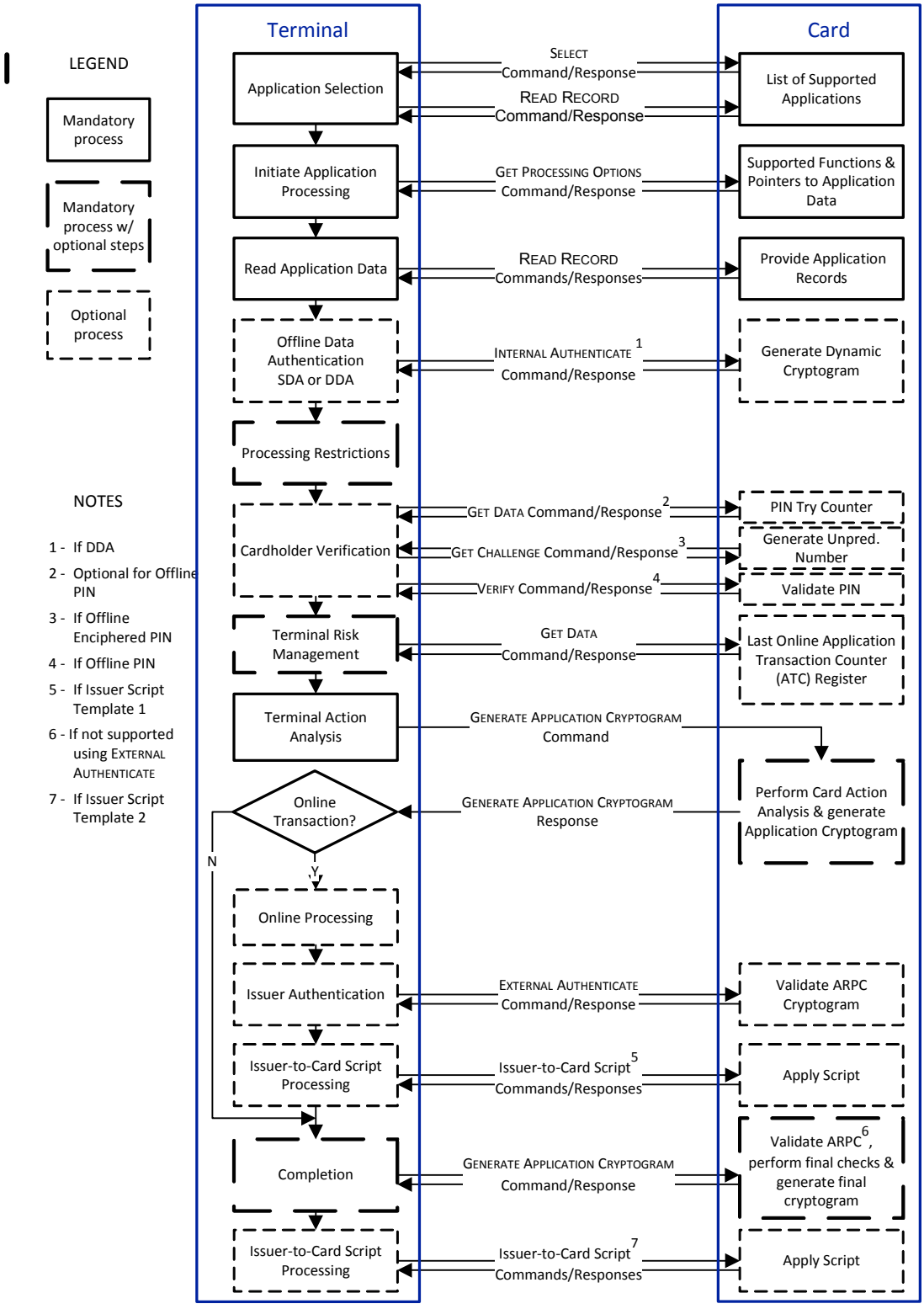
If the terminal transmits a clearing message subsequent to an authorization message, then the TC is transmitted in the clearing message. With single message systems or systems involving acquirer host data capture of approved transactions, the terminal must generate a reversal for issuer-approved transactions which are subsequently declined by the card.

2.1.11 Issuer-to-Card Script Processing

If the issuer includes script updates in the authorization response message, then the terminal passes the script commands to the card, either before or after Completion Processing (as indicated by the issuer script). 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure 2-1: Sample Transaction Flow



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2.2 Mandatory and Optional Functionality

2.2.1 Card Functional Requirements

VIS cards shall support the mandatory functions listed in Table 2-1. Support for conditional functions is required if the associated condition is true. Applications may or may not be capable of optional functions unless support is required by market, regional, or Visa rules. Optional functions that an application is capable of performing are also optional for the issuer unless support is required by market, regional, or Visa rules.

Items marked with (EMV) identify functions where the requirements are the same for EMV and VIS. Items marked with (VIS) identify functions where VIS has a different requirement for support than EMV..

Table 2-1: Card Functional Requirements (1 of 3)

Function	Card Support
Application Selection	Mandatory
• Directory Method	Optional (EMV)
• List of AIDs Method	Mandatory (EMV)
• Partial Name Selection	Mandatory (VIS)
Initiate Application Processing	Mandatory (EMV)
• Profiles Functionality	Optional (VIS)
Read Application Data	Mandatory (EMV)
Offline Data Authentication	Optional (EMV)
• SDA	Optional (EMV)
• DDA	Optional (EMV) Conditional—If CDA supported (VIS)
• CDA	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)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 2-1: Card Functional Requirements (2 of 3)

Function	Card Support
Cardholder Verification	Optional (EMV) Required (VIS)
• Individual CVMs	Optional (EMV) Required (VIS)
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)
• Card Risk Management	Optional (EMV) Mandatory (VIS) Some Card Risk Management steps are optional in VIS. (Refer to Chapter 11, Card Action Analysis.)
• Advice Messages	Optional (EMV)
• Application Cryptogram	Algorithm option provided (EMV) Multiple algorithm options provided (VIS) Mandatory support in card products for algorithms used for CVN 18 and '22', issuers may optionally use other Cryptogram Versions
Online Processing	
• Online Capability	Mandatory (EMV)
• Issuer Authentication	Optional (EMV)
Completion	Mandatory (EMV)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 2-1: Card Functional Requirements (3 of 3)

Function	Card Support
Issuer-to-Card Script Processing	Optional (EMV)
• Secure Messaging	Some form is mandatory if scripts supported (EMV) Recommended form (VIS)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2.2.2 Command Support Requirements

Card support requirements (for the card or application vendor) for the VIS commands is described in Table 2-2.

Note: *Issuers that want to use optional or conditional commands are cautioned to ensure that the card product they choose supports the necessary commands.*

Table 2-2: Command Support Requirements (1 of 2)

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 optional but recommended. CARD BLOCK command is one method (VIS)
EXTERNAL AUTHENTICATE	Conditional—If Issuer Authentication supported using EXTERNAL AUTHENTICATE command (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: Conditional—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)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 2-2: Command Support Requirements (2 of 2)

Command	Card Support
UPDATE RECORD	Optional (VIS)
VERIFY	Conditional—If Offline PIN supported (EMV)

Note: *Even though the Card Status Updates (CSU) sent in the response for Cryptogram Version Number 18 provides functionality equivalent to the APPLICATION BLOCK command, CARD BLOCK command, and unblocking the PIN with the PIN CHANGE/UNBLOCK command, it is still recommended to support the issuer script commands in case the Issuer Authentication cannot be successfully performed to verify the CSU.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

3 Application Selection

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 includes 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 data elements and their usage, see Appendix A, VIS 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 global Visa PIXs are: '1010' Visa Debit or Credit '2010' Visa Electron '3010' Interlink '8010' PLUS The card AID shall 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: 'A0000000031010**01**'—first Visa application (Visa Credit) 'A0000000031010**02**'—second Visa application (for Visa Debit) The AID is used in two different ways: • AID (tag '4F') is used if Directory Selection is supported. • Dedicated File (DF) Name (tag '84'), part of the response to SELECT when an Application Definition File is selected, contains the AID.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

Data Element	Description
Application Definition File (ADF)	A file that is the entry point to application elementary files (AEF) that contain data elements for the application. • File Control Information (FCI) Template – DF Name – FCI Proprietary Template • Application Label • Application Priority Indicator • PDOL • Language Preference (Cards should specify Language Preference in lowercase) • Issuer Code Table Index • Application Preferred Name • FCI Issuer Discretionary Data
Application Elementary Files (AEFs)	Application elementary files contain data elements used by the application in processing.
Application Label, '50'	Mnemonic associated with the 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, '9F12'	Mnemonic associated with the AID. If the Application Preferred Name is present and the Issuer Code Table Index entry is supported by the terminal, then 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, issuers may use this field for their customized brand name recognizable to their customer.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

Data Element	Description
Application Priority Indicator, '87'	Indicates the priority of the given application in a directory and whether the application requires cardholder confirmation to be selected. If the card contains more than one payment account, then the account reflected in the magnetic stripe shall be priority 1.
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 *EMV Book 1*, Annex C.
File Control Information (FCI) Template, 'A5'	Contains information provided in response to the SELECT command. This information varies depending on the type of file selected.
Issuer Code Table Index, '9F11'	Indicates the code table according to ISO/IEC 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 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), '9F38'	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). Use of SFIs is allocated as follows: 1–10 Reserved for EMV 11–20 Payment system specific 21–30 Issuer specific

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Note: *Issuers should expect that EMV-compliant terminals will ignore any historical bytes present in the Answer to Reset (ATR), even if they are ISO-compliant and contain only ISO-defined information. Issuers are free to encode the historical bytes in any way they choose, but are cautioned that unintentional conflict of coding between cards may exist, leading to possible misinterpretation at terminals.*

Neither payment system card personalization checks nor EMVCo type approval testing include tests on the coding or interpretation of historical bytes.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, see Appendix A, VIS Data Element Tables.

Table 3-2: Application Selection—Terminal Data

Data Element	Description
Application Identifier (AID), '9F06'	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 name 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

3.3 Commands

SELECT

The SELECT command shall be performed as described in *EMV Book 1*, section 11.3.

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) 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 the 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 the 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

During Application Selection the READ RECORD command shall be performed as described in *EMV Book 1*, section 11.2.

READ RECORD is used to read the records in the Payment Systems Environment directory (1PAY.SYS.DDF01) 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- **'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 the 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, then 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, then the card shall respond with SW1 SW2 = '6A81'.
   - If there is no PSE, then the card shall respond to the SELECT command from the terminal with SW1 SW2 = '6A82' indicating that this file does not exist.
   - If the PSE is blocked, then the card responds with SW1 SW2 = '6283'.

     Note: *It is not possible for a VIS application to cause the PSE to become blocked.*
   - If the PSE is found, then the card responds to the terminal with SW1 SW2 = '9000' and the FCI for the PSE.
2. If the PSE is found, then 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 shall respond with SW1 SW2 = '6A83' indicating that the record is not available.

   Note: *The PSE personalized for VIS applications shall not contain any DDF entries.*

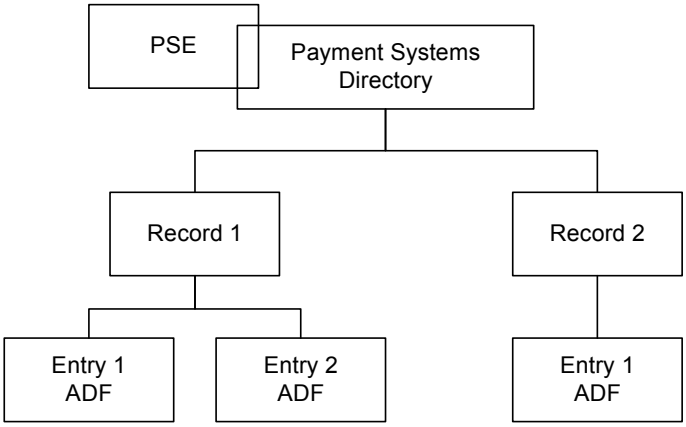
For example, the terminal would perform the following steps to process the Payment Systems Directory shown in Figure 3-1:

1. Reads Record 1 from the Payment Systems Directory.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2. Checks whether the AID for ADF Entry 1 in Record 1 from the Payment System Directory matches a terminal AID. If yes, the ADF is added to the candidate list.
3. Checks whether the AID for ADF Entry 2 in Record 1 from the Payment System Directory matches a terminal AID. If yes, the ADF is added to the candidate list.
4. Reads Record 2 from the Payment Systems Directory.
5. The card responds that there are no more records in the directory.
6. Checks to see whether the AID for ADF Entry 1 in Record 2 from the Payment System Directory matches a terminal AID. If yes, the ADF is added to the candidate list.
7. 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



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 determines whether any card application has a matching AID. (If the card AID is longer than the terminal AID, but the full terminal AID matches the beginning of the card AID, then the card AID shall be considered a match with the terminal AID.)

   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

   a. If the card is blocked or the SELECT command is not supported, then the card shall discontinue processing the command and shall respond with SW1 SW2 = '6A81' indicating that the transaction should be terminated.

   b. If the application is blocked, then the card shall respond with SW1 SW2 = '6283' indicating that application is blocked.

      If the AID matches, then the card shall respond to the SELECT command with the FCI and SW1 SW2 = '9000' (indicating that the application is supported by the card).

      - If the card AID matches the terminal AID except that the card AID is longer, then the card returns the entire card AID (DFname) in the FCI in the SELECT response to the terminal. If there are multiple such matching AIDs, the card chooses which matching card AID to return first.

      If the card does not find a matching AID, then the card shall respond with SW1 SW2 = '6A82' indicating that the application was not found.

2. If the card continues receiving SELECT commands from the terminal, each SELECT command is processed as follows:

   – If the P2 parameter in the SELECT is set to '02' indicating that the card should choose the next application with the same terminal AID:

      - On a multi-application card that could support more than one AID, the card chooses the next application that matches the terminal AID.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - If the application is blocked, then the card shall respond with SW1 SW2 = '6283' indicating that application is blocked.
  - If the application is not blocked, then the card shall respond to the SELECT command with the FCI and SW1 SW2 = '9000' (indicating that the application is supported by the card).

- When the card has no more applications that match the terminal AID, the card shall respond with SW1 SW2 = '6A82' to indicate to the terminal that all matching applications with this AID have been selected.

Otherwise, the card responds as described in step 1b above.

Note: *The terminal continues sending SELECT commands which the card processes as described in this step 2 until the terminal has completed building its candidate list as described in EMV Book 3, section 12.3.3.*

The terminal then proceeds as described in section 3.5 to choose the AID to use for the transaction, and send the final SELECT command to the card.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

3.5 Identifying and Selecting the Application

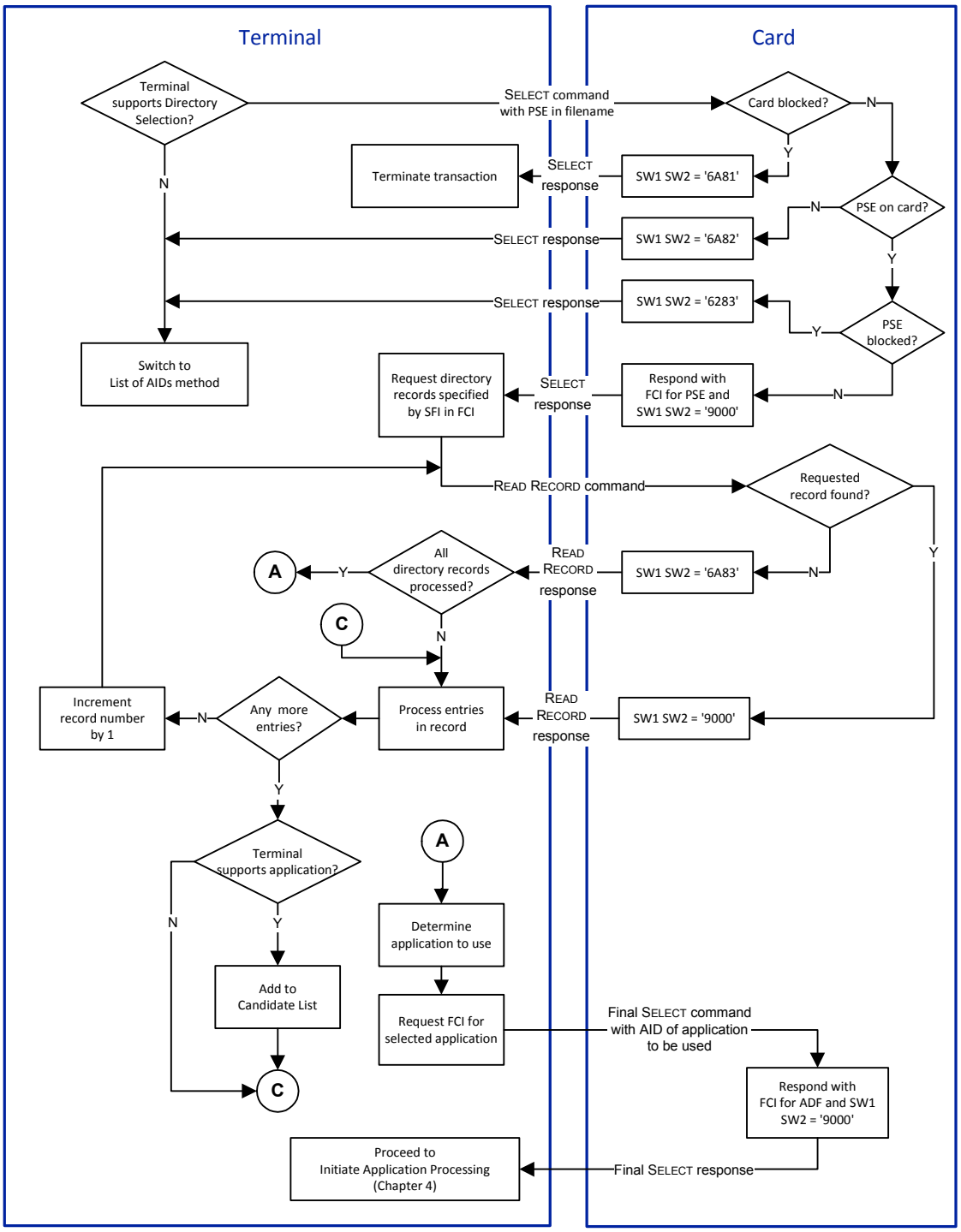
If there is at least one mutually supported application on the candidate list, then the terminal and cardholder determine which application to use. The terminal issues a final SELECT command to the card indicating the application that has been identified for processing the transaction. The card shall respond 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, then the card shall respond with SW1 SW2 = '6283'.

Note: *Issuers should be aware that setting their VIS application to require confirmation by the terminal (see* EMV Book 1*, section 12.4) will mean that the application cannot be selected by a terminal that does not support either Cardholder Confirmation or Cardholder Selection. Single account cards shall not require cardholder confirmation. On a multi-payment card, the primary application (the account that corresponds to the account encoded on the magnetic stripe) shall not require cardholder confirmation.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

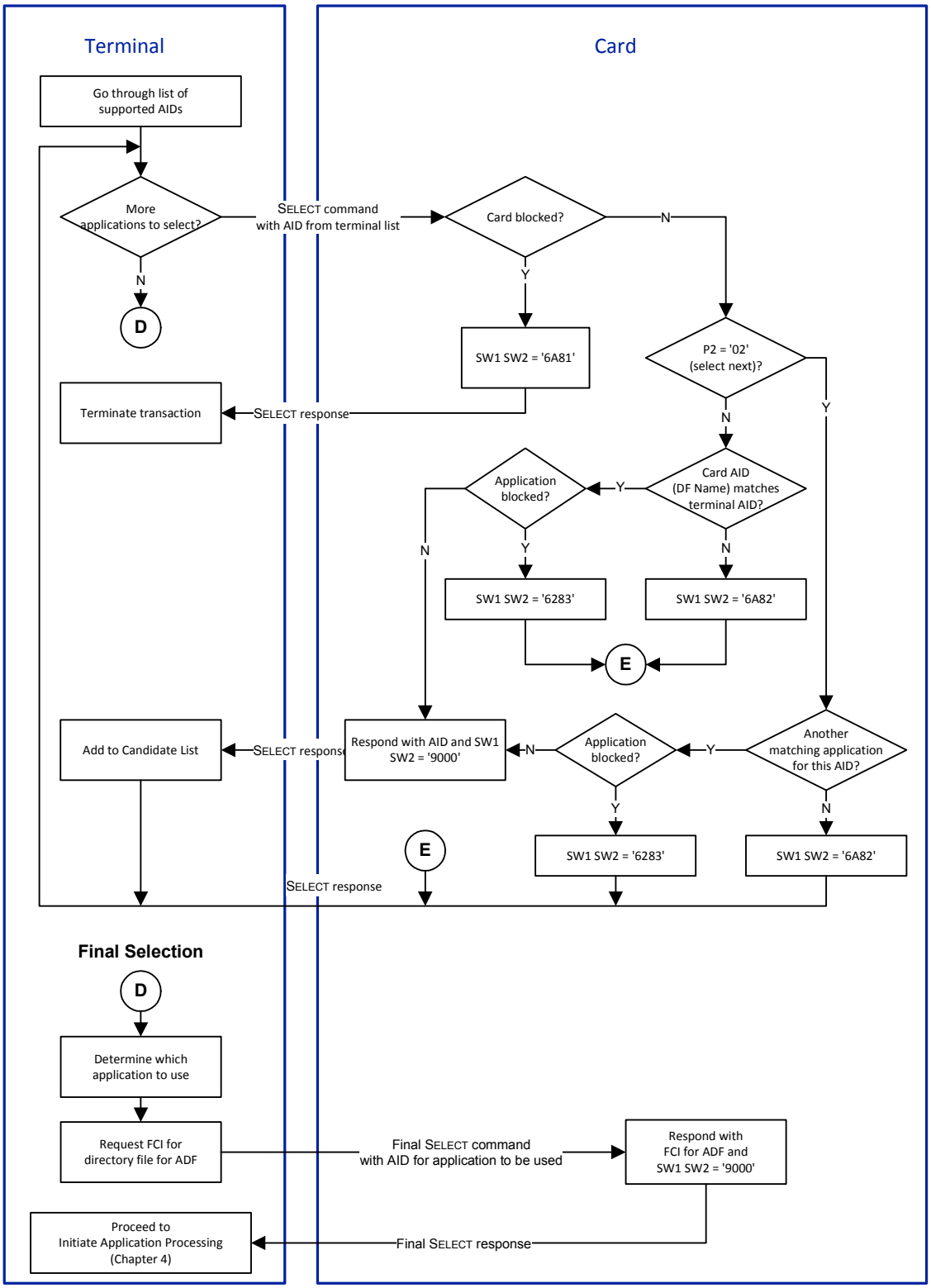
3.6 Flow

Figure 3-2: Application Selection Using Directory Method



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure 3-3: Application Selection Using List of AIDs



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

4 Initiate Application Processing

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 *EMV Book 3*, section 10.1, and *EMV Book 4*, section 6.3.1.

This chapter includes the following sections:

4.1 Card Data
4.2 Terminal Data
4.3 GET PROCESSING OPTIONS Command
4.4 Processing
4.5 Profiles Functionality
4.6 Prior Related Processing
4.7 Subsequent Related Processing

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, VIS Data Element Tables.

Table 4-1: Initiate Application Processing—Card Data (1 of 3)

Data Element	Description
AIP/AFL Entry x (x = 1 to 4), 'DF1x' in 'BF5A'	Identifies the AIP and AFL to be used in a specific transaction environment chosen by the issuer.
Application File Locator (AFL), '94'	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 file label) • 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), '82'	A list that indicates the capability of the card to support specific functions in the application (SDA, DDA, CDA, Terminal Risk Management, Cardholder Verification, and Issuer Authentication using the EXTERNAL AUTHENTICATE command). The AIP shall be personalized in the card to indicate support for Terminal Risk Management and Cardholder Verification. If the card is personalized to allow offline authorization of contact chip transactions, the AIP for contact chip transactions shall be personalized to not support SDA, to support DDA, and may optionally also support CDA. ***Note:*** *A variant of SDA may still be allowed for contactless online transactions with offline data authentication.*
Application Transaction Counter (ATC) '9F36'	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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 4-1: Initiate Application Processing—Card Data (2 of 3)

Data Element	Description
Cryptogram Information Data (CID), '9F27'	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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 4-1: Initiate Application Processing—Card Data (3 of 3)

Data Element	Description
Last Contactless Application Cryptogram Valid Indicator	Indicates whether the last Application Cryptogram generated for the contactless interface is valid for contactless Issuer Update processing. Initiation of a contact transaction invalidates the last contactless Application Cryptogram, so this indicator is reset during Initiate Application processing for contact transactions.
Processing Options Data Object List (PDOL), 9F38'	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).
Profile Control x (x = 1 to 4), 'DF1x' in 'BF59'	Identifies the data and application behavior options supported in a specific transaction environment chosen by the issuer.

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, see Appendix A, VIS Data Element Tables.

Table 4-2: Initiate Application Processing—Terminal Data

Data Element	Description
Data specified in the PDOL	The data from the terminal includes the values for any data element whose tag and length are specified in the card's PDOL.

Note: *If the length of a data element requested by the card using the PDOL is different from the length of that data element in the terminal, the terminal truncates or pads the terminal data according to rules specified in EMV before sending the data to the card. If a data element requested using the PDOL is not present in the terminal, the terminal sends hexadecimal zeros in place of the requested data.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

If the length of data received in the GET PROCESSING OPTIONS command from the terminal is different from the length of data expected by the card, the card shall discontinue processing the GET PROCESSING OPTIONS command and shall return an SW1 SW2 error code to the terminal. The SW1 SW2 error code should be '6985', to cause a return to Application Selection.

The card response shall be in either Format 1 or Format 2 and is described in *EMV Book 3*, section 6.5.8. 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

1. Increment the Application Transaction Counter (ATC) by 1

   If incrementing the ATC results in the ATC being equal to or greater than its maximum value, the application shall be permanently blocked as follows:

   – The application shall discontinue processing the GET PROCESSING OPTIONS command and shall respond with SW1 SW2 = '6985', which permits another application to be selected.

   – All applications linked to this application for application blocking shall also be permanently blocked (respond to SELECT commands with SW1 SW2 = '6283').

   – The application cannot be unblocked by subsequent APPLICATION UNBLOCK commands (see section C.3.1).

   – All applications linked to this application for application blocking also cannot be unblocked by subsequent APPLICATION UNBLOCK commands (see section C.3.1).

   – The application will respond with an error to subsequent SELECT commands (see section 3.3).

   – The application will not generate an Application Cryptogram and will respond with with SW1 SW2 = '6985' to all subsequent GENERATE AC commands (see section C.6.1).

2. The application shall reset data and indicators as follows:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– Reset transient data to zero, see Table A-1.

Note: *Explicit initialization of some card internal data elements listed in this section may not be necessary, if the data element is defined as always calculated or generated by the application, or if the transient nature of those internal data elements results in their already being initialized to the specified value.*

– If the application supports contactless Issuer Update processing, reset the Last Contactless Application Cryptogram Valid Indicator to 0b.

3. Select which AIP and AFL to use for the transaction as determined by Profiles processing, personalization, or proprietary AIP/AFL designation as follows:

   – If the Profiles Functionality is supported (that is, the application is capable of Profiles Functionality and the Profile Selection File is present); the processing described in section 4.5, Profiles Functionality, shall be performed to choose the profile to use for the transaction, which determines the AIP and AFL to return in the GET PROCESSING OPTIONS command response.

   – The card may support proprietary checks to initiate customized processing by designating different AIPs and AFLs for different conditions.

     If both Profiles Functionality and proprietary checks are implemented, the application shall provide a mechanism to disable the proprietary checks so that the Profile Selection functionality may be tested.

   – Either Profile Selection restrictions or proprietary restrictions may result in an error response to the GET PROCESSING OPTIONS command.

4. If there is not an error response required for the GET PROCESSING OPTIONS command, then the card shall respond to the GET PROCESSING OPTIONS command with the AIP and the AFL chosen in step 3.

4.5 Profiles Functionality

Profile Functionality is optional for the implementer and if implemented, is optional for the issuer to support. An application that is capable of Profiles Functionality shall be capable of all features of the Profiles Functionality described in this specification.

Profiles Functionality uses information from the terminal to select different application data and configure different application behavior when the application is used in different transaction environments. For example, Profiles Functionality allows the application to select between multiple AIPs and AFLs personalised on the card when building the response to the GET PROCESSING OPTIONS command, and to configure the card risk management (such as which optional tests to perform, and which counters to use) specific to the transaction environment.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The card uses data from the terminal and internal card data to determine the transaction environment where the card is being used. The issuer determines the transaction environments relevant to the card, and determines what data and behavior should differ for each transaction environment.

Profiles Functionality consists of two main components:

- Profile Selection - choosing which profile to use for a specific transaction
- Profile Behavior - choosing what data and behavior are used depending on the chosen profile.

Profile Selection is a mechanism used to identify the transaction environment, and select which Profile to use for the transaction. The data needed from the terminal for the application to identify the transaction environment is requested using the PDOL sent from the card to the terminal in the final SELECT response. This data is returned from the terminal to the card in the GET PROCESSING OPTIONS command data field.

Profiles Behavior uses a Profile Control data element to configure the application data and behavior specific to the chosen profile.

If an issuer wants to use Profiles Functionality, the issuer shall select an application capable of Profiles Functionality, personalize the data needed to select which profile to use, and configure the application data and behavior for the transaction. If all these requirements are met, then Profiles Functionality is supported.

Sections 4.5.1 and 4.5.2 apply only when Profiles Functionality is supported.

4.5.1 Profile Selection

The application uses the PDOL to request that the terminal send data in the GET PROCESSING OPTIONS command data field.

The application uses the content of the GPO command data, internal card data, and the Profile Selection Entries to select the Profile ID for the Profile to use for the transaction. The Profile ID identifies a Profile Control to use for the transaction that specifies how application data and behavior are to be configured for transactions that use the Profile.

Profile Selection File Processing may also cause the card to discontinue processing the command and respond with a status word indicating an error, allowing the terminal to return to Application Selection to select another application.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

After receiving a GET PROCESSING OPTIONS command from the terminal, the card performs the Profile Selection processing as described in section E.1, Profile Selection, to determine the Profile to use for the transaction.

- If there is an error in processing the Profile Selection File, or Profile Selection processing does not result in a valid Profile Control being chosen for the transaction; then the card shall respond to the GET PROCESSING OPTIONS command with SW1 SW2 = '6985' (Conditions of use not satisfied), indicating that the terminal shall remove the application from the candidate list and may return to Application Selection to select another application.
- If Profile Selection processing results in selection of a valid Profile ID for the transaction, the Profile Control chosen for the transaction shall be Profile Control x, where x = the value of Profile ID resulting from the Profile Selection Processing described in section E.1.

4.5.2 Profile Behavior for Initiate Application Processing

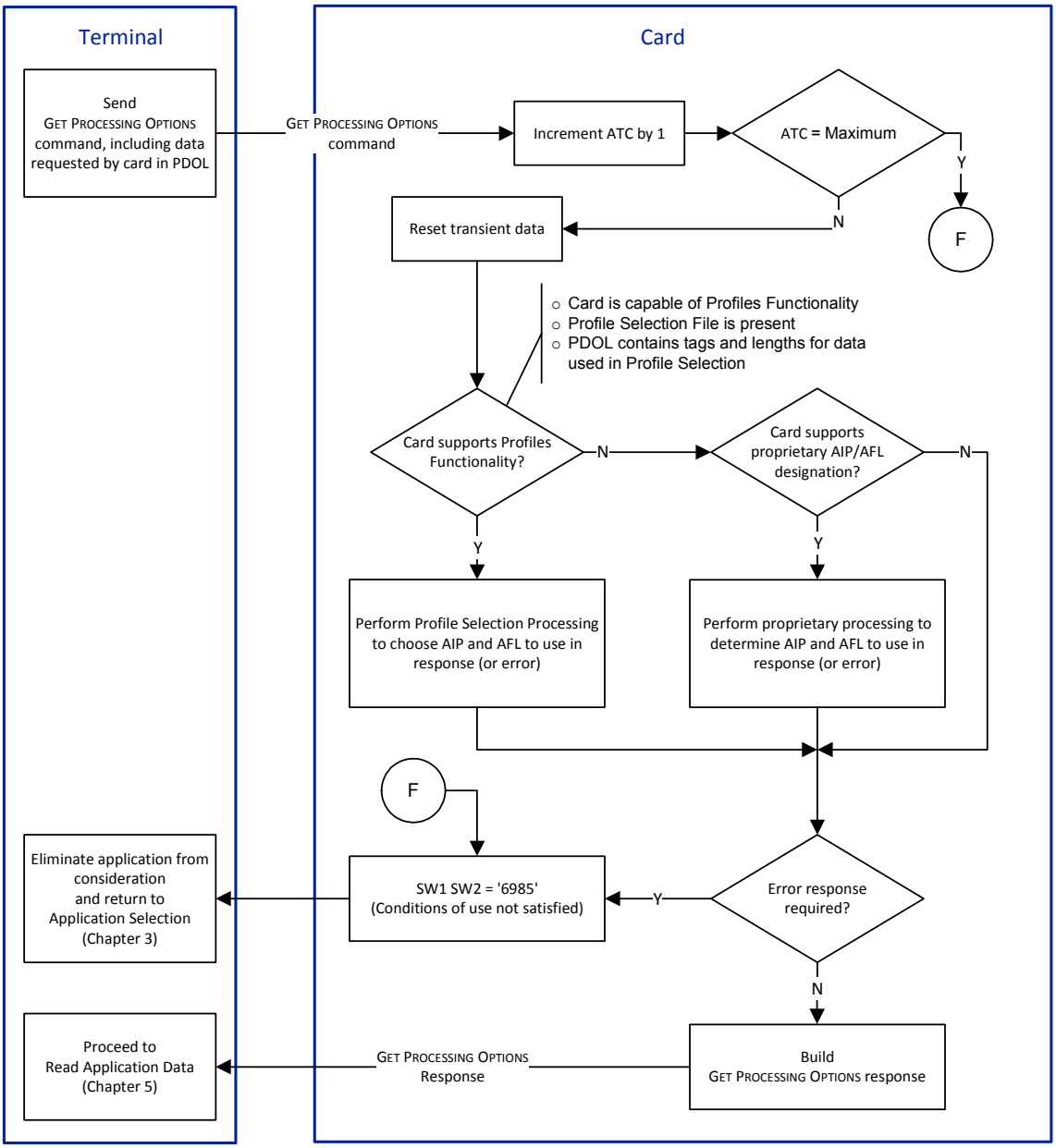
Profile-specific data and behavior are configured using the Profile Control chosen for the transaction.

For Initiate Application Processing, the Profile Control chosen for the transaction identifies the values for the AIP and AFL to be returned to the terminal in the GPO response. The application uses the AIP and AFL values in the AIP/AFL Entry y (where y = the AIP/AFL Entry ID in bits 8-5 of the Profile Control chosen for the transaction).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

Figure 4-1: Initiate Application Processing Flow



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

4.6 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.

4.7 Subsequent Related Processing

Application Selection

If Profiles Functionality did not choose a valid Profile Control for the transaction or other restrictions applied and control was returned to Application Selection, then 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 whether the card supports Cardholder Verification.

Card Action Analysis

If the Profiles Functionality is supported, the card uses the Profile Control chosen for the transaction to customize the data and behavior for Card Action Analysis.

The terminal uses the AIP provided by the card in response to the GET PROCESSING OPTIONS command to determine whether the card supports CDA.

Online Processing

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Completion Processing

If the Profiles Functionality is supported, the card uses the Profile Control chosen for the transaction to customize the data and behavior for Completion Processing.

The terminal uses the AIP provided by the card in response to the GET PROCESSING OPTIONS command to determine whether the card supports CDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

5 Read Application Data

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

Read Application Data shall be performed as described in *EMV Book 3,* section 10.2.

This chapter includes 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

5.1 Card Data

For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 5-1: Read Application Data—Card Data

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. The records read for offline data authentication shall be TLV-coded with tag equal to '70'. For files with SFI in the range of 1-10, the record tag ('70') and record length are not included in the data to be authenticated. For files with SFI in the range of 11-30, the record tag ('70') and the record length are included in the data to be authenticated.
Application File Locator (AFL), '94'	During the Initiate Application Processing function, the card sends the terminal the AFL which contains an entry for each group of records to be read by the terminal during Read Application Data. Each entry in the AFL 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 SDA, DDA, and CDA. See EMV Book 3, section 10.2 for details on coding of the entries in the AFL.
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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 *EMV Book 3*, section 6.5.11.

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 from the card's Application Elementary Files 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 file designated in the AFL 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

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 and CDA.

Processing Restrictions

The terminal uses data (such as the Application Expiration Date) that is read during Read Application Data.

Cardholder Verification

The terminal uses data (such as the CVM List) that is read during Read Application Data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Terminal Risk Management

The terminal uses data (such as the Lower Consecutive Offline Limit) that is read during Read Application Data.

Terminal Action Analysis

The terminal uses data (such as the Issuer Action Codes) that is read during Read Application Data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6 Offline Data Authentication

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 and CDA)

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.

Dynamic data authentication can be either DDA or CDA. During DDA and CDA processing the terminal authenticates the static card data and also authenticates a cryptogram that the card generates using transaction-unique data. DDA and CDA ensure that issuer-selected card data elements have not been altered since the card was personalized. DDA and CDA also confirm 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 *EMV 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.

If the card is personalized to allow offline authorization of contact chip transactions, the card is personalized to not support SDA, to support DDA, and may optionally also support CDA.

This chapter includes the following sections:

6.1 Keys and Certificates
6.2 Card Data
6.3 Terminal Data
6.4 Determining Whether to Perform SDA, DDA, or CDA
6.5 Static Data Authentication (SDA)
6.6 Dynamic Data Authentication (DDA and CDA)
6.7 Prior Related Processing
6.8 Subsequent Related Processing

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 (recovered) for validation and data recovery. For additional information on the RSA algorithm, refer to *EMV 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/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 *EMV 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, DDA, and CDA)
- Issuer Public/Private Keys (SDA, DDA, and CDA)
- ICC Public/Private Keys (DDA and CDA)

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 are used to sign Issuer Public Keys. The same Visa public/private key pairs are used for SDA, DDA, CDA, and Offline Enciphered PIN.

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

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.1.2.2 Issuer Public/Private Keys

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

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. The Issuer PK Certificate is created by signing the Issuer Public Key input file with the Visa CA Private Key.

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.
- 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*.

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

The format of the data recovered from Issuer PK Certificate is shown in *EMV Book 2*, Table 5. 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 *EMV Book 2*, Table 2.

All cards which support SDA, DDA, or CDA 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 SDA, DDA, and CDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.1.2.3 ICC Public/Private Keys

For cards supporting DDA or CDA, 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 *EMV Book 2*, Table 12. 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 shall 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 *EMV Book 2*, Table 14.

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 Card Data

The terminal uses the card data elements described in Table 6-1 in Offline Data Authentication processing or in processing related to SDA, DDA, or CDA processing. For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 6-1: Offline Data Authentication—SDA, DDA and CDA Card Data (1 of 6)

Data Element	Description
Application Interchange Profile (AIP), '82'	Contains indicators showing the offline data authentication methods supported by the card: • SDA supported • DDA supported • CDA supported This data element is used for SDA, DDA and CDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 6-1: Offline Data Authentication—SDA, DDA and CDA Card Data (2 of 6)

Data Element	Description
Certificate Authority Public Key Index (PKI), '8F'	Provided by the CA with the Issuer PK Certificate. It identifies the payment system public key in the terminal to use for verifying the Issuer PK Certificate. This data element is used for SDA, DDA and CDA.
Card Verification Results (CVR)	Contains the following: • 'Offline static data authentication failed on last transaction and transaction declined offline'—an indicator that is set during Card Action Analysis of subsequent transactions showing that SDA failed on a previous offline-declined transaction. • 'Offline dynamic data authentication failed on last transaction and transaction declined offline'—an indicator that is set during Card Action Analysis of subsequent transactions showing that DDA or CDA failed on a previous offline-declined transaction. • 'Offline dynamic data authentication performed'—an indicator that is set either during offline dynamic data authentication or during Card Action Analysis of the current transaction showing that DDA or CDA was performed on the current transaction. This data element is used internal to the card for SDA, DDA and CDA, and is not passed to the terminal as part of processing the INTERNAL AUTHENTICATE command.
Dynamic Data Authentication Failure Indicator	Indicates that DDA or CDA 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. This data element is not used for SDA, is used internal to the card for DDA and CDA, and is not passed to the terminal as part of processing the INTERNAL AUTHENTICATE command.
Dynamic Data Authentication Data Object List (DDOL), '9F49'	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'). The DDOL is required to be present on all cards that support DDA This data element is used for DDA and is not used for SDA and CDA.
ICC Dynamic Data	Issuer-specified data elements to be included in the Signed Dynamic Application Data. EMV mandates that the ICC Dynamic Number be the first data element of the ICC Dynamic Data. This data element is used for DDA and CDA and is not used for SDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 6-1: Offline Data Authentication—SDA, DDA and CDA Card Data (3 of 6)

Data Element	Description
ICC Dynamic Number	Part of the ICC Dynamic Data containing a time-variant number generated by the ICC. Visa mandates that the Application Transaction Counter (ATC) be the first data element of the ICC Dynamic Number. The ATC in ICC Dynamic Number may be in plaintext, or (if business needs require) it may be encrypted. This data element is used for DDA and CDA and is not used for SDA.
ICC Private Key	The key used to encrypt the Signed Dynamic Application Data. This data element is not used for SDA, is used internal to the card for DDA and CDA, and is not passed to the terminal as part of processing the INTERNAL AUTHENTICATE command.
ICC Public Key (PK) Certificate, '9F46'	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 section 6.1.2.3. 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, then multiple ICC PK Certificates shall 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 section 4.4, Processing, for additional information. If any of the signed data elements can be changed post-issuance, then the capability to change the ICC Public Key Certificate and the hash of static data within it shall also be supported. This data element is used for DDA and CDA and is not used for SDA.
ICC Public Key Exponent, '9F47'	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). Visa recommends using the value 3. This data element is used for DDA and CDA and is not used for SDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 6-1: Offline Data Authentication—SDA, DDA and CDA Card Data (4 of 6)

Data Element	Description
ICC Public Key Remainder, '9F48'	The portion, if any, of the ICC Public Key that does not fit into the ICC Public Key Certificate. This data element is used for DDA and CDA and is not used for SDA.
Issuer Public Key Certificate, '90'	The certificate containing the Issuer Public Key that has been signed with the Visa CA Private Key. This certificate is described in section 6.1.2.2. This data element is used for SDA, DDA and CDA.
Issuer Public Key Exponent, '9F32'	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). Visa recommends using the value 3. This data element is used for SDA, DDA and CDA.
Issuer Public Key Remainder, '92'	The portion, if any, of the Issuer Public Key that does not fit into the Issuer PK Certificate. This data element is used for SDA, DDA and CDA.
Registered Application Identifier (RID) portion of the Application Identifier (AID)	The RID is registered with the International Organisation for Standardisation (ISO) and identifies the payment system specific list of public keys that is stored in the terminal. Visa's RID is 'A000000003'. This data element is used for SDA, DDA and CDA.
Signed Dynamic Application Data, '9F4B'	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 *EMV Book 2*, Table 16. This data element is used for DDA and CDA and is not used for SDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 6-1: Offline Data Authentication—SDA, DDA and CDA Card Data (5 of 6)

Data Element	Description
Signed Static Application Data (SAD), '93'	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 *EMV Book 2*, Table 6. The format of the data elements to be hashed are in *EMV Book 2*, Table 3. The following data elements are recommended for inclusion in the signature generation: • 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') • Card Risk Management Data Object List 1 (CDOL1) • Card Risk Management Data Object List 2 (CDOL2) The following data elements shall be included in the signature generation if offline data authentication is supported: • SDA Tag List ('9F4A') if offline data authentication is supported • Application Interchange Profile if offline data authentication is supported ***Note:*** *The order for data input to SDA is dependent on the order of the data in records, as described in* EMV Book 3*, section 10.3.* ***Note:*** *Regional requirements may require certain data to be signed. Contact your regional representative for more information.* If the signed data is not unique within the application, then multiple SADs shall 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 section 4.5, Profiles Functionality and section E.2, Profile Behavior, for an explanation of Profiles Functionality and how different data can be specified for different transaction environments. If the card supports the ability to change any of the signed data elements after the card has been issued to the cardholder, then the capability to change the SAD shall also be supported. ***Note:*** *If any of the signed data elements are modified using an issuer script, then the SAD must also be updated (or SDA will fail).* This data element is used for SDA and is not used for DDA or CDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 6-1: Offline Data Authentication—SDA, DDA and CDA Card Data (6 of 6)

Data Element	Description
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. This data element is used for SDA, DDA and CDA.
SDA Tag List, '9F4A'	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 shall be included in the SDA Tag List if SDA, DDA, or CDA is supported. This data element is used for SDA, DDA and CDA.

Offline Data Authentication—DDA and CDA Terminal Data

6.3 Terminal Data

The card uses no terminal data during SDA. The card uses the data from the terminal, described in Table 6-2, during DDA and CDA processing. For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 6-2: Offline Data Authentication—DDA and CDA Terminal Data

Data Element	Description
Unpredictable Number , '9F37'	This data is included in the INTERNAL AUTHENTICATE command for DDA, and in the GENERATE AC command for CDA.
Default Dynamic Data Object List (Default DDOL)	A terminal data element that contains only the Unpredictable Number, and that is used as the DDOL if the card does not contain a DDOL. ***Note:*** *A DDOL is required for all cards that support DDA.*

Note: *If the length of a data element requested by the card using a DOL is different from the length of that data element in the terminal, the terminal truncates or pads the terminal data according to the rules specified in EMV before sending the data to the card. If a data element requested using a DOL is not present in the terminal, the terminal sends hexadecimal zeros in place of the requested data.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.4 Determining Whether to Perform SDA, DDA, or CDA

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, DDA, or CDA.

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

If the terminal determines that both the card (as indicated by the AIP) and the terminal support CDA, then it performs CDA. Otherwise, if both support DDA, then the terminal performs DDA. Otherwise, if both card and terminal support SDA, then the terminal performs SDA.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.5 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.

No commands are used in SDA processing.

6.5.1 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 *EMV Book 2*, section 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 SDA 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, then SDA has passed.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.6 Dynamic Data Authentication (DDA and CDA)

During dynamic data authentication 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: DDA and CDA. With both, the terminal validates that static card data has not been altered and also validates a dynamic cryptogram generated by the card. With 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 CDA, the card responds to the first GENERATE AC command received during Card Action Analysis (and if requested, also to the second GENERATE AC command received during Completion) 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 DDA.

Note: *CDA is described in the EMV specifications. It is optional in VIS (as it is in EMV), and is not discussed in detail in this document. For more information, see the EMV specifications and bulletins.*

6.6.1 Commands

6.6.1.1 INTERNAL AUTHENTICATE Command

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

If the length of data received in the INTERNAL AUTHENTICATE command from the terminal is different from the length of data expected by the card, the card shall discontinue processing the INTERNAL AUTHENTICATE command and shall return an SW1 SW2 error code to the terminal. The SW1 SW2 error code should be '6700' (Wrong Length).

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. Either Format 1 or Format 2 shall be used for the response data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.6.1.2 GENERATE APPLICATION CRYPTOGRAM (AC) Command

The terminal issues the first GENERATE AC command during Card Action Analysis processing. The transaction is eligible for CDA if bit 5 of the P1 byte is set to 1b, indicating that a CDA signature is requested by the terminal.

If the transaction is eligible for CDA, then a TC or ARQC returned by the card shall be contained within a cryptographic envelope as described in *EMV Book 2*, section 6.6.1. See Chapter 11, Card Action Analysis, for additional information on this command.

6.6.2 Processing

During offline dynamic data authentication 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 offline dynamic data authentication processing is the generation of the dynamic signature.

DDA and CDA processing are described in more detail in *EMV Book 2*, section 6, *EMV Book 3*, section 10.3, and *EMV Book 4*, section 6.3.2. The following sections provide an overview of the DDA and CDA processes. For detailed information about CDA, see the EMV specifications and bulletins.

6.6.2.1 DDA

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

4. Dynamic Signature Generation (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 of the CVR to 1b.

      Note: *Instead of using the CVR bit as an indicator, implementations may instead set an internal application indicator for the above listed condition if the specified CVR bit is set to the required value during Card Risk Management processing in the Card Action Analysis for the same transaction.*

   b. Concatenate the terminal data received in the INTERNAL AUTHENTICATE command and the card data specified in the ICC Dynamic Data with other data. *EMV Book 2*, Table 15, 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 (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, then DDA has passed.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.6.2.2 CDA

CDA requires the following processing:

- The terminal performs Steps 1 to 3 of DDA processing after Read Application Data and prior to Terminal Action Analysis.
- The remaining card step of CDA 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, Card Action Analysis. This inclusion of the Application Cryptogram in a dynamic signature only occurs when the transaction is eligible for CDA as shown in the GENERATE AC command and the Application Cryptogram is an ARQC or TC.
- The remaining terminal step of CDA is the validation of the dynamic signature which occurs during Online Processing. If the validation of the dynamic signature fails, then the transaction is declined offline by the terminal.
- When CDA is requested in the first GENERATE AC, it also may be requested in the second GENERATE AC according to the rules in Chapter 13.

6.7 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 or CDA, 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 (SDA) Tag List.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

6.8 Subsequent Related Processing

Terminal Action Analysis

The terminal uses SDA, DDA, and CDA 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 CDA is requested by the terminal, then 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 1b, then the card sets the 'Offline dynamic data authentication failed on last transaction and transaction declined offline' bit of the CVR to 1b. A similar bit is set if the Static Data Authentication Failure Indicator is set to 1b.

If the current transaction is declined offline and the 'Offline dynamic data authentication failed' bit of the TVR received from the terminal is set to 1b, then the card sets the Dynamic Data Authentication Failure Indicator to 1b. A similar indicator is set for SDA.

Online Processing

If CDA is requested by the terminal and the card response to the first GENERATE AC is a TC or ARQC, then the terminal recovers and validates the data in the RSA signature envelope in the GENERATE AC response.

Completion

The Static Data Authentication Failure Indicator and Dynamic Data Authentication Failure Indicator are reset to 0b 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 (the Issuer Authentication Indicator is not present).

If the current transaction is declined offline and the 'CDA failed' bit of the TVR received from the terminal is set to 1b, then the card sets the Dynamic Data Authentication Failure Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

7 Processing Restrictions

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 *EMV Book 3*, section 10.4, and *EMV Book 4*, section 6.3.3 and Annex A.

This chapter includes the following sections:

7.1 Card Data
7.2 Terminal Data
7.3 Processing
7.4 Prior Related Processing
7.5 Subsequent Related Processing

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 7-1: Processing Restrictions—Card Data

Data Element	Description
Application Effective Date, '5F25'	The Application Effective Date is the date when the application becomes activated for use.
Application Expiration Date, '5F24'	The Application Expiration Date is the date after which the application is no longer available for use.
Application Version Number, '9F08'	This data element 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 150.
Application Usage Control (AUC), '9F07'	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, '5F28'	This Issuer Country Code is the EMV-defined data element indicating the country of the card issuance. It is used in Application Usage Control checking by the terminal.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 7-2: Processing Restrictions—Terminal Data

Data Element	Description
Application Version Number, '9F09'	This data element indicates the version of the application in the terminal.
Transaction Type, '9C'	This data element indicates the type of financial transaction. (It is represented by the first two digits of ISO 8583-1987, Processing Code.) It is used in Application Usage Control checking by the terminal.
Terminal Country Code, '9F1A'	This data element indicates the country where the terminal is located. It is used in Application Usage Control checking by the terminal.
Transaction Date, '9A'	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 whether they are the same. If the Application Version Numbers are not the same, then the terminal sets the ‘ICC and terminal have different application versions’ bit of the TVR to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

7.3.2 Application Usage Control

During Application Usage Control, the terminal checks various conditions at the point of transaction to determine whether to set a bit in the TVR. The TVR bit settings are subsequently checked in Terminal Action Analysis to determine whether to decline the transaction offline or send the transaction online. If the Application Usage Control (AUC) and the Issuer Country Code were received from the card during Read Application Data, then 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, then the transaction is considered domestic for AUC processing. If the transaction is domestic, then, in the AUC from the card, the domestic indicator corresponding to Transaction Type must be 1b to indicate that the requested service is allowed.

   For example, if the transaction is a cash transaction, then the 'Valid for domestic cash transactions' bit of the AUC must be 1b for the transaction to be allowed to continue.

   International

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

   For example, if the transaction is a cash transaction, then the 'Valid for international cash transactions' bit of the AUC must be 1b for the transaction to be allowed to continue.

2. ATM Checking

   If the card acceptance device is an ATM, then the 'Valid at ATMs' bit of the AUC must be 1b for the transaction to be allowed to continue. If the card acceptance device is not an ATM, then the 'Valid at terminals other than ATMs' bit of the AUC must be 1b for the transaction to be allowed to continue.

   If any of the above checks performed by the terminal fail, then the terminal sets the 'Requested service not allowed for card product' bit of the TVR to 1b and continues processing the transaction.

   Note: *If the 'Requested service not allowed for card product' bit of the TVR is set to 1b during Processing Restrictions, the corresponding bit in the Visa-required TAC-Denial will cause the terminal to request a transaction decline as a result of Terminal Action Analysis.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 1b, then that usage or capability is supported.

Table 7-3: Application Usage Control (AUC)

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Usage
1	1b	x	x	x	x	x	x	x	Valid for domestic cash transactions
1	x	1b	x	x	x	x	x	x	Valid for international cash transactions
1	x	x	1b	x	x	x	x	x	Valid for domestic goods
1	x	x	x	1b	x	x	x	x	Valid for international goods
1	x	x	x	x	1b	x	x	x	Valid for domestic services
1	x	x	x	x	x	1b	x	x	Valid for international services
1	x	x	x	x	x	x	1b	x	Valid at ATMs
1	x	x	x	x	x	x	x	1b	Valid at terminals other than ATMs
2	1b	x	x	x	x	x	x	x	Domestic cashback allowed
2	x	1b	x	x	x	x	x	x	International cashback allowed

Note: *An EMV terminal does not differentiate between goods and services (see EMV Application Note No. 27). In Application Usage Control, the value of 'Valid for domestic goods' must be the same as the value of 'Valid for domestic services', and the value of 'Valid for international goods' must be the same as the value of 'Valid for international services'.*

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, then the terminal sets the 'Application not yet effective' bit of the TVR to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

7.3.4 Application Expiration Date

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, then the terminal sets the 'Expired application' bit of the TVR to 1b.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

8 Cardholder Verification

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 *EMV Book 3*, section 10.5, and *EMV Book 4*, section 6.3.4.

This chapter includes 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

8.1 Card Data

The terminal uses the data from the card, described in Table 8-1, during CVM List processing. For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 8-1: CVM List Processing—Card Data (1 of 5)

Data Element	Description
Application Currency Code, '9F42'	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, then Application Currency Code shall be present. Used by the terminal during CVM List Processing.
Application Currency Exponent, '9F44'	Indicates the implied position of the decimal point from the right for amounts in the designated currency for the application. May be used by the terminal during CVM List Processing.
Application Default Action (ADA), '9F52'	Contains issuer-specific indicators for the card action for exception conditions.
Application Interchange Profile (AIP), '82'	Contains an indicator showing whether the card supports cardholder verification. This indicator shall be set to 1b. Used by the terminal during CVM List 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 Used by the terminal during Offline PIN Processing. ***Note:*** *Instead of using the CVR bits as indicators, implementations may instead set internal application indicators for the above listed conditions if the specified CVR bits are set to the required values during Card Risk Management processing in the Card Action Analysis for the same transaction.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 8-1: CVM List Processing—Card Data (2 of 5)

Data Element	Description
Cardholder Verification Method (CVM) List, '8E'	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 unattended cash • If manual cash • If purchase with 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.* Used by the terminal during CVM List Processing. See section 8.4.1 for an example of coding a CVM List.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 8-1: CVM List Processing—Card Data (3 of 5)

Data Element	Description
Certificate Authority Public Key Index (PKI), '8F'	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 shall be used to recover the Issuer PK Certificate. Used by the terminal during Offline Enciphered PIN Processing.
ICC PIN Encipherment or ICC Public Key (PK) Certificate, '9F2D' or '9F46'	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 *EMV Book 2*, Table 22. May be used by the terminal during Offline Enciphered PIN Processing.
ICC PIN Encipherment or ICC Public Key Exponent, '9F2E' or '9F47'	Contains the exponent used in the algorithm that enciphers the PIN for Offline Enciphered PIN. Shall be 3 or (2^{16} + 1). Visa recommends using the value 3. May be used by the terminal during Offline Enciphered PIN Processing.
ICC PIN Encipherment or ICC Public Key Remainder, '9F2F' or '9F48'	Contains the portion, if necessary, of the public key that does not fit into the ICC's public key certificate. May be used by the terminal during Offline Enciphered PIN Processing.
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. May be used by the terminal during Offline Enciphered PIN Processing.
Issuer Public Key (PK) Certificate, '90'	Signed with the Visa Private Key. Contains the public key to be used to decipher the ICC PIN Encipherment or ICC PK Certificate. May be used by the terminal during Offline Enciphered PIN Processing.
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 SDA, DDA and CDA. (See Chapter 6, Offline Data Authentication.) Used by the terminal during Offline Enciphered PIN Processing.
Issuer Public Key Exponent, '9F32'	Contains the exponent used in the algorithm that deciphers the ICC PIN Encipherment or ICC PK Certificate. Shall be 3 or (2^{16} + 1). Visa recommends using the value 3. May be used by the terminal during Offline Enciphered PIN Processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 8-1: CVM List Processing—Card Data (4 of 5)

Data Element	Description
Issuer Public Key Remainder, '92'	Contains the portion, if necessary, of the Issuer Public Key that does not fit into the Issuer PK Certificate. May be used by the terminal during Offline Enciphered PIN Processing.
PIN Try Limit	Issuer-specified maximum number of consecutive incorrect PIN tries allowed. Used by the terminal during Offline PIN Processing.
PIN Try Counter, '9F17'	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. Used by the terminal during Offline PIN Processing.
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, then 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. Used by the terminal during Offline PIN Processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 8-1: CVM List Processing—Card Data (5 of 5)

Data Element	Description
Registered Application Provider Identifier (RID)	The part of the Application Identifier (AID) that identifies the Application Provider (payment system). The RID and the PKI are used to identify the Visa Public Key to be used to recover the Issuer PK Certificate. Used by the terminal during Offline Enciphered PIN Processing.

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 and CDA. 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 8-1.

8.2 Terminal Data

The terminal uses the terminal data, described in Table 8-2, during PIN processing. For a detailed description of the data element and its usage, see Appendix A, VIS Data Element Tables.

Table 8-2: PIN Processing—Terminal Data

Data Element	Description
Transaction PIN, '99'	Data entered by the cardholder for the purpose of PIN verification.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, then 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

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
- 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 8-3 could be used.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 8-3: 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 unattended cash	
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	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

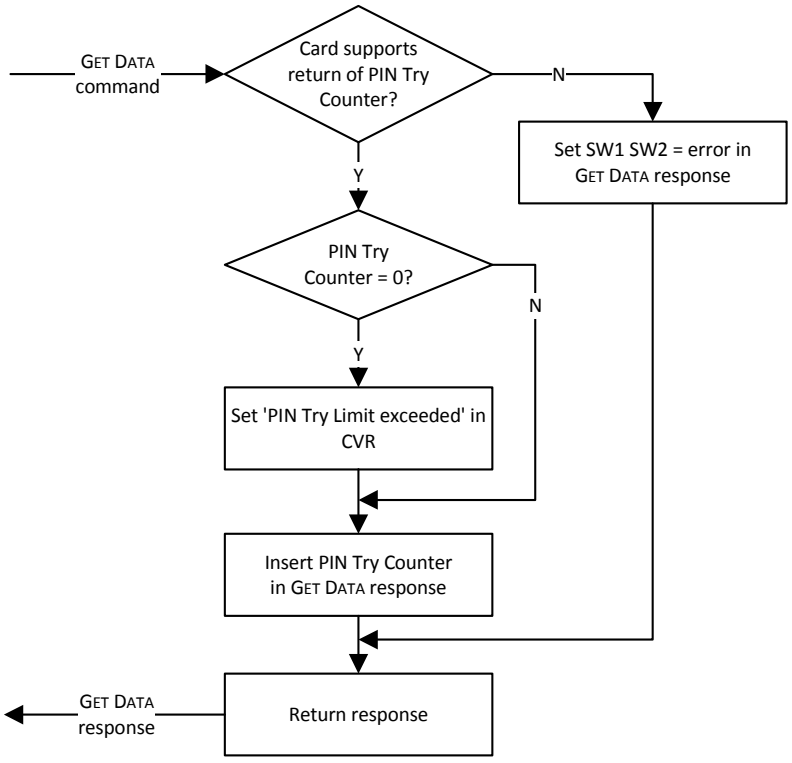
   After the terminal determines that an offline PIN is to be entered, the terminal may transmit a GET DATA command to the card to retrieve the PIN Try Counter.

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

      - If the PIN Try Counter is zero, set the 'PIN Try Limit exceeded' bit of the CVR to 1b.
      - 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, then 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

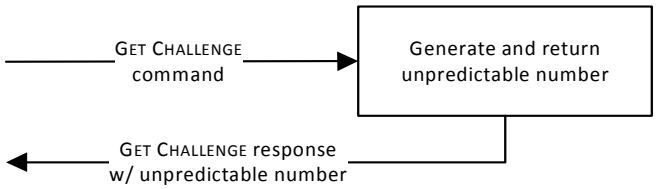


Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

2. PIN Encipherment

   If the CVM is Offline Enciphered PIN, then 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 the 'Offline PIN verification performed' bit of the CVR to 1b.

   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 proceed to the PIN verification step.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, then the card shall:

      - Set the ‘PIN Try Limit exceeded’ bit of the CVR to 1b
      - Set the ‘Offline PIN verification failed’ bit of the CVR to 1b
      - 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. Compare Transaction PIN to Reference PIN

      If the PIN try function is not blocked, the card shall decrement the PIN Try Counter by one. Then the card shall:

      - If the PIN is in the clear, compare the Transaction PIN to the Reference PIN.
      - If the PIN is enciphered and there is no new random challenge available from a GET CHALLENGE command immediately prior to this VERIFY command, return SW1 SW2 = '6984' in the VERIFY response.
      - If the PIN is enciphered and there is a new random challenge available from a GET CHALLENGE command immediately prior to this VERIFY command, 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 EMV Book 2, section 7. Then the card shall compare the deciphered Transaction PIN to the Reference PIN.

        Note: *The processing described in EMV Book 2, section 7, includes verification that the challenge recovered from the VERIFY command matches the challenge sent by the card in the GET CHALLENGE response immediately before the VERIFY command.*

   c. Matching PINs

      If they match, then the card shall:

      - Reset the PIN Try Counter to the PIN Try Limit value
      - Set the ‘Offline PIN verification failed’ bit of the CVR to 0b
      - Return a VERIFY command response indicating that the command was successfully executed (SW1 SW2 = '9000').

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

d. Non-Matching PINs

If the Transaction PIN does not match the Reference PIN or there was an error during PIN decipherment, then the card shall set the 'Offline PIN verification failed' bit of the CVR to 1b.

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

- If the PIN Try Counter is zero (no PIN tries remaining, then the card shall:
  - Set the 'PIN Try Limit exceeded' bit of the CVR to 1b
  - If the 'If PIN Try Limit exceeded on current transaction, block application' bit of the ADA is 1b, then set the 'Application blocked by card because PIN Try Limit exceeded' bit of the CVR to 1b and block the application. The card shall allow the current transaction to proceed through Completion. If the application is blocked by this method, then the card shall respond to the GENERATE AC command with an AAC. 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')
- If the PIN Try Counter is greater than zero (PIN Tries Remaining):
  - If PIN verification failed because of an error during PIN decipherment, then the card shall return a VERIFY command response indicating an error. The recommended error is SW1 SW2 = '6983' or '6984' (this can prevent the PIN Try counter from being decremented to zero, thereby blocking the PIN, when the actual failure is a PIN decipherment failure).
  - Otherwise, if the resulting value of the PIN Try Counter is not zero, then the card shall return a VERIFY response indicating the remaining number of PIN tries (SW1 SW2 = '63Cx' where x equals the remaining PIN tries).

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, then the card shall:

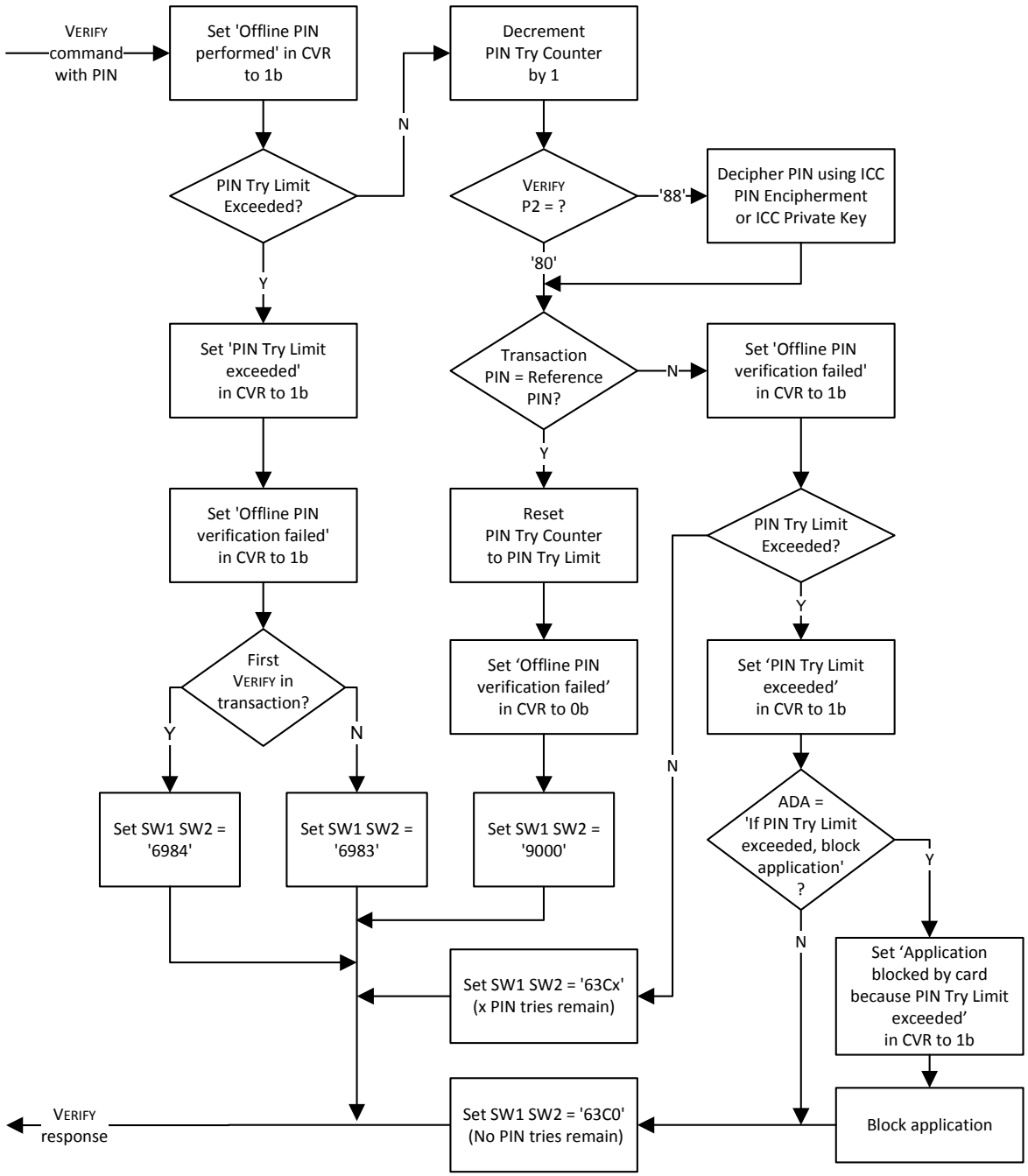
– Reset the PIN Try Counter to the value of the PIN Try Limit

– Set the 'Offline PIN verification failed' bit of the CVR to 0b.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure 8-3: Offline PIN Processing



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 ADA parameters 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, then the enciphered PIN is included in the online request. If the CVM is Offline PIN, then 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, then the card uses ADA parameters to determine whether to decline the transaction.

If the transaction successfully went online and Issuer Authentication passed for Cryptogram Version Number 18, then the Card Status Updates (CSU) in the online response can be used to reset the PIN Try Counter to an issuer-specified value sent in the CSU.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

9 Terminal Risk Management

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 *EMV Book 3*, section 10.6, and *EMV Book 4*, section 6.3.5.

This chapter includes the following sections:

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 9-1: Terminal Risk Management—Card Data

Data Element	Description
Application Interchange Profile (AIP), '82'	Contains an indicator showing whether the card supports Terminal Risk Management. This indicator shall be set to 1b.
Application Primary Account Number (PAN), '5A'	The cardholder account number for the application
Application Transaction Counter (ATC), '9F36'	A counter of transactions initiated since the application was personalized on the card. Maintained by the application on the card.
Last Online Application Transaction (ATC) Register, '9F13'	ATC value of the last online authorization where Issuer Authentication requirements were satisfied. If the card mandates Issuer Authentication, then the register is reset to the value of the ATC during Completion if Issuer Authentication is performed and passes. If Issuer Authentication is optional or not supported, then the register 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, then the transaction is declined offline. It is used in terminal velocity checking and required for terminal new card checking.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 9-2: Terminal Risk Management—Terminal Data

Data Element	Description
Amount, Authorized, '9F02'	This numeric data element 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, '9F1B'	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), '95'	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 (in Terminal)	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. This transaction log maintained by the terminal is different from the Transaction Log that may be supported in the card as described in Appendix I, Transaction Log.
Transaction Status Information (TSI), '9B'	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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, then 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, then 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, then 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 Lower and Upper 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: *EMV also requires that the Lower and Upper Consecutive Offline Limits (tags '9F14' and '9F23' respectively) be personalized on the card if the terminal is to perform the New Card Check.*

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

10 Terminal Action Analysis

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 *EMV Book 3*, section 10.7, and *EMV Book 4*, section 6.3.6.

This chapter includes 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

10.1 Card Data

The terminal uses the card data elements described in Table 10-1 in Terminal Action Analysis or during Request Cryptogram Processing. These data elements were previously read from the card during Read Application Data. For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 10-1: Terminal Action Analysis—Card Data

Data Element	Description
Card Risk Management Data Object List 1 (CDOL1), '8C'	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 section D.3.1, Data Input for CVN 10 ('0A') and section D.4.1, Data Input for CVN 18 ('12') and CVN '22', for cryptogram CDOL1 requirements. Chapter 11, Card Action Analysis, shows the CDOL1 requirements for Card Action Analysis.
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 1b if the corresponding TVR condition is to result in the action designated by the IAC. The three IACs are: • IAC—Denial, '9F0E" The issuer sets the IAC bits to 1b that correspond to the TVR bits for conditions which the issuer wishes to result in an offline decline. • IAC—Online, '9F0F' The issuer sets the bits to 1b that correspond to the TVR bits for conditions which the issuer would like to result in an online authorization. • IAC—Default, '9F0D' The issuer sets the bits to 1b 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.

Note: *The cryptogram algorithms defined in Appendix D do not use the Transaction Certificate Data Object List (TDOL). For proprietary cryptograms see EMV Book 3, section 9.2.2 for more information on use of a TDOL.*

Section 10.4.1 contains an example of how the IACs and TACs are used with the Terminal Verification Results (TVR) to determine transaction disposition.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Note: *Setting any of the following bits in the IACs or TACs will not influence the outcome of the transaction, because the associated TVR bits will never be set at the times the terminal compares the IACs and TACs to the TVR:*

- *Issuer Authentication was unsuccessful*
- *Issuer Script processing failed before final GENERATE AC command*
- *Issuer Script processing failed after final GENERATE AC command*

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

10.2 Terminal Data

For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables, the *Visa Transaction Acceptance Device Requirements* and the *Visa Transaction Acceptance Device Guide*.

The terminal uses the terminal data elements described in Table 10-2 during Terminal Action Analysis or Request Cryptogram Processing.

Table 10-2: Terminal Action Analysis—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 the card's IACs, the TAC bits are set to 1b 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 the *Visa Transaction Acceptance Device Requirements*.
Terminal Data Elements	The terminal data elements specified in the CDOL1 or TDOL from the card are included in the GENERATE AC command.

Note: *The cryptogram algorithms defined in Appendix D do not use a TDOL or TC Hash Value. For proprietary cryptograms see EMV Book 3, section 9.2.2 for more information on use of these data elements.*

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 CDA. *EMV Book 3*, Table 12, shows the coding of this parameter. The data portion of the command contains the terminal data objects requested in the CDOL1, which was received from the card during Read Application Data.

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

10.4 Processing

10.4.1 Review Offline Processing Results

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

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

The terminal may review offline processing results after Terminal Risk Management, or earlier in order to eliminate the need for unnecessary processing. For example, Terminal Action Analysis could be performed after Static Data Authorization (SDA) to eliminate the need for Cardholder Verification when SDA failure results in an offline decline.

During processing the terminal compares bits in the IACs and TACs to the corresponding bits in the Terminal Verification Results (TVR). If corresponding bits in the TVR and the IAC or TAC are both set to 1b, the disposition for the IAC or TAC is used.

Section 10.4.1.1 illustrates how the comparisons work.

10.4.1.1 IAC Usage Example

The issuer wishes to send transactions online if Offline DDA fails or if the PIN Try Limit is exceeded, so the IAC—Online bits from the card are set as below:

		Offline DDA Failed ↓		PIN Try Limit Exceeded ↓		
IAC—Online	**00001000b**	**00000000b**	**00100000b**	**00000000b**	**00000000b**

The terminal records offline processing results in the TVR. In the following transactions, the application is expired. In Transaction 2, Offline DDA has also failed.

Transaction 1: The application is expired so the TVR is set to:

		Expired Application ↓			
TVR	**00000000b**	**01000000b**	**00000000b**	**00000000b**	**00000000b**
IAC—Online	**00001000b**	**00000000b**	**00100000b**	**00000000b**	**00000000b**

The terminal will not request to go online here because the TVR and IAC—Online have no corresponding bits that are set to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Transaction 2: Offline DDA has failed and the application is expired so the TVR is set to:

	Offline DDA Failed ↓	Expired Application ↓			
TVR	00001000b	01000000b	00000000b	00000000b	00000000b
IAC—Online	00001000b	00000000b	00100000b	00000000b	00000000b

Offline DDA Failed is set to '1' in the IAC—Online and the TVR so the terminal will request to send the transaction online.

Similar comparisons are done with the other IACs and the TACs.

10.4.1.2 Terminal IAC and TAC Processing Steps

The processing steps taken by the terminal are:

1. The terminal compares the IAC—Denial to the TVR.
   If no IAC—Denial is present, then the terminal uses a default value of '0000000000'.

   If any corresponding bits in the IAC—Denial and the TVR are both set to 1b, then the terminal:

   – Sets the Authorization Response Code to “Z1” (Offline Decline).

   – Proceeds to request an Application Authentication Cryptogram (AAC) Application Cryptogram (for an offline decline).

2. The terminal does a similar compare with the TAC—Denial and the TVR.
   If no TAC—Denial is present, then the terminal uses a default value of '0000000000'.

   If any corresponding bits are both set to 1b, then the same actions as done for the IAC—Denial should be performed.

3. If the terminal has online capabilities, then it compares the IAC—Online and TAC—Online to the TVR.
   If no IAC—Online is present, then the terminal uses a default value of '1111111111'.
   If no TAC—Online is present, then the terminal uses a default value of '0000000000'.

   If any corresponding bits in the IAC—Online and TVR are both set to 1b, then the terminal:

   – Proceeds to request an Authorization Request Cryptogram (ARQC) Application Cryptogram to go online for authorisation.

4. If the terminal does not have online capabilities, then it compares the IAC—Default and the TAC—Default to the TVR.
   If no IAC—Default is present, then the terminal uses a default value of '1111111111'.
   If no TAC—Default is present, then the terminal uses a default value of '0000000000'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If any corresponding bits are both set to 1b, then the terminal:

– Sets the Authorization Response Code to “Z3” (Offline Decline Unable To Go Online).

– Proceeds to request an AAC Application Cryptogram (for an offline decline).

5. If none of the previous compares found corresponding bits which were both set to 1b, then the terminal:

   – Sets the Authorization Response Code to “Y1” (Offline Approve).

   – Proceeds to request a Transaction Certificate (TC) Application Cryptogram (for an offline approval).

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 (as described in Chapter 11).

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11 Card Action Analysis

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 chapter include checking:

- Activity on previous transactions
- Whether the 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 both the card and the terminal support Combined DDA/AC Generation (CDA), where the card returns an ARQC or TC as part of a dynamic signature, the terminal may request CDA.

Card Action Analysis shall be performed as described in *EMV Book 3*, section 10.8.

This chapter includes the following sections:

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 data elements and their usage, see Appendix A, VIS Data Element Tables. For an overview of the types of counters used in VIS, please see Appendix G, Overview of Velocity-Checking Counters.

Table 11-1: Card Action Analysis—Card Data (1 of 8)

Data Element	Description
Application Cryptogram, '9F26'	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, '9F51'	A code indicating the domestic currency associated with the application.
Application Default Action (ADA), '9F52'	Contains issuer-specific indicators for the card action for exception conditions.
Application Interchange Profile (AIP), '82'	Contains indicators showing the capability of the card to support CDA, and Issuer Authentication using the EXTERNAL AUTHENTICATE command.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (2 of 8)

Data Element	Description
Card Risk Management Data Object List 1 (CDOL1), '8C'	List of data elements (tags and lengths) to be passed to the card application with the first GENERATE AC command. The tags and lengths for the following data elements shall be included in CDOL1 if the Application Cryptogram is generated using Cryptogram Version Number 10, 18,or '22' (CVN 10, CVN 18, or CVN '22'): • Amount, Authorized • Amount, Other • Terminal Country Code • Terminal Verification Results (TVR) • Transaction Currency Code • Transaction Date • Transaction Type • Unpredictable Number If not already included in CDOL1 for cryptogram generation, the tags and lengths of the following data elements shall also be present in CDOL1 if the listed Card Risk Management check is to occur: • Transaction Currency Code—Velocity Checking for Total Consecutive Offline International transactions (Based on Currency), Velocity Check for Total Transaction Amount • Terminal Country Code—Velocity Checking for Total Consecutive International Transactions (Based on Country) • Amount, Authorized—Velocity Checking for Total Transaction AmountAmount • Terminal Verification Results (TVR)—SDA, DDA, or CDA Failed on Last Transaction Tags for any of the data elements that are already included in the CDOL1 as part of the terminal data used for cryptogram generation should not be repeated in CDOL1 for use in the card risk management check. The tags and lengths of data elements needed for logging transactions internal to the card during first GENERATE AC processing should also be included in CDOL1. The tag for Unpredictable Number shall be included in the CDOL1 when CDA is supported.
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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (3 of 8)

Data Element	Description
Consecutive Transaction Counter (CTC), 'DF11' in 'BF56'	A Visa proprietary counter that is incremented for each offline approved (and optionally for each declined) transaction.
Consecutive Transaction Counter Limit (CTCL), '9F58', or 'DF21' in 'BF56'	Visa proprietary data element indicating the maximum number of consecutive offline transactions allowed before an online authorization is requested. *Renamed from Lower Consecutive Offline Limit ('9F58')*
Consecutive Transaction Counter International (CTCI), 'DF11' in 'BF57'	A Visa proprietary counter that is incremented for each offline approved (and optionally for declined) transaction which is either not in the card's designated currency and if currency conversion is supported is also not in a designated alternate currency, or optionally is not in the issuers country.
Consecutive Transaction Counter International Limit (CTCIL) , '9F53', or 'DF21' in 'BF57'	The number of offline international transactions allowed (where the transactions are in a currency other than the card's designated currency or a supported conversion currency, or optionally in a country other than the issuer's country) before online processing is requested.
Consecutive Transaction Counter International Country (CTCIC), 'DF51' in 'BF57'	Visa proprietary counter that is incremented for each offline approved (and optionally for declined) transaction where the Issuer Country Code differs from the Terminal Country Code.
Consecutive Transaction Counter International Country Limit (CTCICL), '9F72', or 'DF61' in 'BF57'	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.
Consecutive Transaction Counter x (CTC x), 'DF1x' in 'BF56' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTC x: CTC 1, CTC 2, CTC 3, CTC 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTC x in the Profile.
Consecutive Transaction Counter Limit x (CTCL x), or 'DF2x' in 'BF56' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCL x: CTCL 1, CTCL 2, CTCL 3, CTCL 4. Each CTCL x is used as the upper limit for the corresponding CTC x.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (4 of 8)

Data Element	Description
Consecutive Transaction Counter International x (CTCI x), 'DF1x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCI x: CTCI 1, CTCI 2, CTCI 3, CTCI 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTCI x in the Profile.
Consecutive Transaction Counter International Limit x (CTCIL x), 'DF2x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCIL x: CTCIL 1, CTCIL 2, CTCIL 3, CTCIL 4. Each CTCIL x is used as the lower limit for the corresponding CTCIC x.
Consecutive Transaction Counter International Country x (CTCIC x), 'DF5x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCIC x: CTCIC 1, CTCIC 2, CTCIC 3, CTCIC 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTCIC x in the Profile.
Consecutive Transaction Counter International Country Limit x (CTCICL x), 'DF6x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCICL x: CTCICL 1, CTCICL 2, CTCICL 3, CTCICL 4. Each CTCICL x is used as the lower limit for the corresponding CTCICL x.
Contactless Transaction Counter (CLTC), 'DF11' in 'BF55'	A Visa proprietary counter that is incremented for each offline contactless domestic transaction.
Contactless Transaction Counter Lower Limit (CLTCLL), 'DF21' in 'BF55'	The number of offline contactless domestic transactions allowed before online processing is requested.
Conversion Currency Code x *for minimum implementations of currency conversion, x = 1 to 5*	A code identifying an alternate currency to be converted to the Application Currency for multiple currency velocity checking.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (5 of 8)

Data Element	Description
Cryptogram Information Data (CID), '9F27'	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) • Advice required and a reason code for the advice Sent to the terminal in the GENERATE AC response.
Cumulative Total Transaction Amount (CTTA), 'DF11' in 'BF58'	Visa proprietary data element specifying the cumulative amount of offline approved transactions in the designated currency (Application Currency Code) plus the approximate value of offline approved transactions in any alternate currency that was converted to the the designated currency since the counter was reset.
Cumulative Total Transaction Amount Limit (CTTAL), '9F54' or DF21' in 'BF58'	Visa proprietary data element specifying the limit on the total amount of offline approved transactions in either the designated currency (Application Currency Code) or in any alternate currency that was converted to an approximate value in the designated currency since the counter was reset. If exceeded, online processing is requested.
Cumulative Total Transaction Amount x (CTTA x), 'DF1x' in 'BF58' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTTA x: CTTA 1, CTTA 2, CTTA 3, CTTA 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTTA x in the Profile.
Cumulative Total Transaction Amount Limit x (CTTAL x), 'DF2x' in 'BF58' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTTAL x: CTTAL 1, CTTAL 2, CTTAL 3, CTTAL 4. Each CTTAL x is used as the lower limit for the corresponding CTTA x.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (6 of 8)

Data Element	Description
Currency Conversion Factor x *for minimum implementations of currency conversion, x = 1 to 5*	A decimal value used in the currency conversion algorithm to convert the value of an amount in the Conversion Currency to the designated currency in which the account is managed (identified by the Application Currency Code). This converted value is only used for comparisons and incrementing counters. The Amount, Authorized remains in the Transaction Currency. The Currency Conversion Factor x may be updated using an Issuer Script Command to the Currency Conversion Parameters data element. Because this rate is intended to be an approximation, update should not be necessary unless major currency fluctuations occur.
Currency Conversion Parameters , '9F73'	A constructed data element listing the currencies that may be used for currency conversion and the associated conversion rate for each currency. Currency. Consists of one to five convertible currency entries. Each convertible currency entry consists of a Conversion Currency Code x and the associated Currency Conversion Factor x (the values of “x” match). The Currency Conversion Factor x is used to approximate the value of a transaction in a designated alternate currency (Conversion Currency x) converted to the designated currency in which the account is managed (Application Currency). ***Note:*** *The “x” is not related to Profiles Functionality, it is used to associate the Currency Conversion Factor x with the Conversion Currency Code x for which the factor is used.*
Dynamic Data Authentication Failure Indicator	An internal application indicator that is set when DDA or CDA 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, '9F56'	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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (7 of 8)

Data Element	Description
Issuer Script Command Counter	An internal application counter used to count Issuer Script Commands as follows: • If the counter is not cyclic: – it counts the number of Issuer Script commands containing secure messaging that were received by the card since the counter was last reset – the counter may be reset during completion – when the counter has reached the maximum value, this 4-bit counter remains set to 'F'. • If the counter is cyclic: – it counts Issuer Script commands that were successful – it counts continuously without resetting – when the counter has reached the maximum value, this 4-bit counter rolls over from 'F' to '0'.
Issuer Script Failure Indicator	An internal application indicator that is set when Issuer Script processing fails, and is reset during Completion of an online transaction where issuer authentication requirements are met.
Last Online ATC Register, '9F13'	ATC value of the last transaction that was authorized online and satisfied Issuer Authentication requirements.
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.
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, '9F17'	Number of PIN tries remaining.
Profile Control x, 'DF1X' in 'BF59' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, a data element that indicates the profile-specific data and behavior options chosen by the issuer to be used for transactions processed using the profile identified by Profile ID = x. The Profile Control x associated with the Profile ID chosen during Initiate Application Processing is referred to as “the Profile Control chosen for the transaction”.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-1: Card Action Analysis—Card Data (8 of 8)

Data Element	Description
Profile ID	If Profiles Functionality is supported, an identifier selected during Initiate Application Processing to identify the profile to be used for processing transactions that take place in an issuer-defined transaction environment.
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.
VLP Available Funds, '9F79' or 'DF51' in 'BF55'	Amount remaining for low-value offline contactless transactions.
VLP Funds Limit, '9F77' or 'DF71' in 'BF55'	The issuer limit for VLP Available Funds.
VLP Reset Threshold or 'DF61' in 'BF55'	The minimum value to which VLP Available Funds is allowed to be decremented before the card requests online processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 their tag and length were included in the CDOL1 read from the card during Read Application Data. The CDOL1 requirements for the Card Risk Management checks and cryptogram generation 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 data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 11-2: Card Action Analysis—Terminal Data

Data Element	Description
Amount, Authorized, '9F02'	The amount of the transaction.
Terminal Country Code, '9F1A'	Terminal data indicating the country of the terminal. This data element is requested by the card in the CDOL1.
Terminal Verification Results (TVR), '95'	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.
Transaction Currency Code, '5F2A'	A code that indicates the currency of the transaction. This data element is requested by the card in the CDOL1.
Transaction Type, '9C'	Indicates the type of financial transaction.

Note: *If the length of a data element requested by the card using the CDOL1 is different from the length of that data element in the terminal, the terminal truncates or pads the terminal data according to rules specified in EMV before sending the data to the card. If a data element requested using CDOL1 is not present in the terminal, the terminal sends hexadecimal zeros in place of the requested data.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 CDA. *EMV Book 3*, Table 12, shows the format of P1. The data portion of the command contains the data requested in the CDOL1.

The transaction is eligible for CDA when the GENERATE AC command requests CDA in the 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 CDA and the cryptogram type is a TC or ARQC, then the cryptogram returned is in an RSA public key envelope as described in *EMV 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.

If the application is permanently blocked because the ATC has reached its maximum value, the card does not generate an Application Cryptogram or dynamic signature, discontinues processing the GENERATE AC command, and returns SW1 SW2 = '6985' (see section C).

Note: *A permanently blocked application should not receive any GENERATE AC commands.*

If the application is blocked, but the ATC has not yet reached its maximum value, the card should skip the Card Risk Management processing described in sections section 11.4.2, Card Risk Management Overview and section 11.4.3, Card Risk Management Checks; and shall decline the transaction by returning an AAC type Application Cryptogram.

If the length of data received in the GENERATE AC command from the terminal is different from the length of data expected by the card, the card should discontinue processing the GENERATE AC command and should return an SW1 SW2 error code to the terminal. The SW1 SW2 error code should be '6700' (Wrong Length).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.2 Card Risk Management Overview

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, then 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), then the card shall proceed to the next step in card risk management. If the Application Default Action (ADA) is not personalized in the card, then the card shall use a default value of all zeros.

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

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

Risk Management Check	Section	Requirement	Result (If condition occurs)
Issuer Script Processed on Last Online Transaction	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 or Profile Control for the transaction setting determines whether this failure results in online processing.
Velocity Checking for Consecutive Transactions Lower Limit	11.4.3.6	Optional	If limit is exceeded, requests online processing and sets a CVR indicator.
Velocity Checking for Consecutive International Transactions Lower Limit	11.4.3.7	Optional	If limit is exceeded, requests online processing and sets a CVR indicator.
Velocity Checking for Consecutive International Country Transactions Lower Limit	11.4.3.8	Optional	If limit is exceeded, requests online processing and sets a CVR indicator.
Velocity Checking for Cumulative Total Transaction Amount Lower Limit	11.4.3.9	Optional	If limit is exceeded, requests online processing and sets a CVR indicator. This check supports currency conversion.
Velocity Checking for Contactless Offline Transactions Lower Limit	11.4.3.10	Optional	If limit is exceeded, requests online processing and sets a CVR indicator.
Velocity Checking for VLP Contactless Transactions Reset Threshold	11.4.3.11	Optional	If limit is exceeded, requests online processing and sets a CVR indicator.
New Card	11.4.3.12	Optional	Sets CVR indicator if no transactions have been processed online. ADA or Profile Control for the transaction setting determines whether this condition results in online processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 11-3: Card Risk Management Checks (3 of 3)

Risk Management Check	Section	Requirement	Result (If condition occurs)
Offline PIN Verification Not Performed (PIN Try Limit Exceeded)	11.4.3.13	Optional	Sets CVR indicator if Offline PIN Verification was not performed and the PIN Try Limit was previously exceeded. ADA or Profile Control for the transaction setting determines whether this results in an offline decline or online processing.
Go Online on Next Transaction From Previous Online Response	11.4.3.14	Conditional	Requests online processing if the issuer response for a previous online transaction requested the card to go online for future transactions.
Deleted: Special Transactions	*11.4.3.15*		
PIN Verification Not Performed or Not Successful for a PIN-Expecting Card	11.4.3.16	Optional	Requests online processing if a PIN-Expecting card does not receive the VERIFY command
VERIFY Not Received by PIN-Expecting Card	11.4.3.17	Optional	Sets CVR indicator

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3 Card Risk Management Checks

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

11.4.3.1 Online Authorization Not Completed

This conditional check is required if Issuer Authentication is supported (the Issuer Authentication Indicator is present) 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 1b in a previous transaction when an online authorization is requested (see Chapter 13, Completion Processing, for conditions under which this indicator is reset).

If the indicator is set, then 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 1b, then the card:

- Sets the Online Requested by Card Indicator to 1b.
- Sets the ‘Last online transaction not completed’ bit of the CVR to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

This check is mandatory if Issuer Authentication is supported (the Issuer Authentication Indicator is present). 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, then online processing is requested by the card.

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

- Sets the 'Issuer Authentication failure on last online transaction' bit of the CVR to 1b.
- Sets the internal Online Requested by Card Indicator to 1b if either of the following is true:
  - Profiles Functionality is not supported and the 'If Issuer Authentication failure, transmit next transaction online' bit of the Application Default Action (ADA) is 1b, .
  - Profiles Functionality is supported and the 'If Issuer Authentication failure, transmit next transaction online' bit of the Profile Control chosen for the transaction is 1b.

11.4.3.3 Static Data Authentication (SDA) Failed on Last Transaction

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

If the Static Data Authentication Failure Indicator is 1b, then the card sets the 'Offline static data authentication failed on last transaction and transaction declined offline' bit of the CVR to 1b.

11.4.3.4 Offline Dynamic Data Authentication (DDA or CDA) Failed on Last Transaction

This check is mandatory if DDA or CDA is supported. It checks whether DDA or CDA failed on a previous offline declined transaction.

If the Dynamic Data Authentication Failure Indicator is 1b, then the card sets the 'Offline dynamic data authentication failed on last transaction and transaction declined offline' bit of the CVR to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 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 1b, then the card sets the 'Issuer Script processing failed' bit of the CVR to 1b.

The card shall set the Online Requested by Card Indicator to 1b if the Issuer Script Failure Indicator is set to 1b and either of the following is true:

- Profiles Functionality is not supported and the 'If Issuer Script failed on a previous transaction, transmit transaction online' bit of the ADA is set to 1b.
- Profiles Functionality is supported and the 'If Issuer Script failed on a previous transaction, transmit transaction online' bit of the Profile Control chosen for the transaction is set to 1b.

Note: *If the 'Issuer Script processing failed' bit is set in the CVR of the first GENERATE AC response, the script that failed was performed during a previous transaction and the indicator has not yet been reset.*

11.4.3.6 Velocity Checking for Consecutive 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.

If Profiles Functionality is not supported and the Consecutive Transaction Counter (CTC) and Consecutive Transaction Counter Limit (CTCL) are present, then the card shall perform the following check:

- the card checks whether the sum of the CTC plus one is greater than the CTCL if *either* of the following is true:
  - the 'Do not count declined transactions' bit of the ADA is set to 0b
  - the terminal requested an approval (TC) or an online authorization (ARQC)

  Otherwise the card checks whether the CTC is greater than the CTCL

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If Profiles Functionality is supported and the Consecutive Transaction Counter x and Consecutive Transaction Counter Limit x are present; then the card shall perform the following check for each Consecutive Transaction Counter x:

- the card checks whether the sum of the Consecutive Transaction Counter x plus one is greater than the Consecutive Transaction Counter Limit x if *both* of the following are true:
  - the 'Allow Counting in CTC x' bit of the Profile Control for the transaction is set to 1b
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC) or an online authorization (ARQC)

  Otherwise the card checks whether the Consecutive Transaction Counter x is greater than the Consecutive Transaction Counter Limit x if *either* of the following is true:
  - the 'Allow Counting in CTC x' bit of the Profile Control for the transaction is set to 1b
  - the 'Check limits for CTC x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card:

- Sets the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Sets the Online Requested by Card Indicator to 1b to request that an ARQC should be returned after completion of Card Risk Management.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.7 Velocity Checking for Consecutive International Transactions Lower Limit

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 any supported currency on the card. An issuer option allows this check to extend the definition of international transaction to also include any transaction where the Terminal Country Code does not match the Issuer Country Code (even if the currency is supported).

Note: *When Profiles Functionality is supported, the counter may be checked against the limit even though the transaction is in the Application Currency or in currency that can be converted.*

When Profiles Functionality is not supported, the counter is checked against the limit only if the transaction is in an international currency that cannot be converted to the application currency.

If Profiles Functionality is not supported and the Application Currency Code, Consecutive Transaction Counter International (CTCI), and Consecutive Transaction Counter International Limit (CTCIL) are present; and if Consecutive International Transactions card velocity checking includes international country transactions, the Issuer Country Code is present; then the card shall perform the following check:

- the card shall check whether the sum of the CTCI plus one is greater than the CTCIL if *both* of the following are true:
  - *either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
    - the Terminal Country Code does not match the Issuer Country Code and the ‘CTCI also counts non-matching country code transactions’ bit of the ADA is set to 1b
  - *either* of the following is true:
    - the ‘Do not count declined transactions’ bit of the ADA is set to 0b
    - the terminal requested an approval (TC) or online authorization (ARQC)

  Otherwise, the card shall check whether the CTCI is greater than the CTCIL if either of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b

If Profiles Functionality is supported and the Application Currency Code, Consecutive Transaction Counter International x, and Consecutive Transaction Counter International Limit x are present; and if Consecutive International Transactions card velocity checking includes international country transactions, the Issuer Country Code is present; then the card shall perform the following check for each Consecutive Transaction Counter International x:

- The card checks whether the sum of the Consecutive Transaction Counter International x plus one is greater than the Consecutive Transaction Counter International Limit x if *all* of the following are true:
  - the 'Allow Counting in CTCI x' bit of the Profile Control for the transaction is set to 1b
  - *either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
    - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC) or online authorization (ARQC)

  Otherwise, the card checks whether the Consecutive Transaction Counter International x is greater than the Consecutive Transaction Counter International Limit x if *either* of the following is true:
  - the 'Allow Counting in CTCI x' bit of the Profile Control for the transaction is set to 1b
  - the 'Check limits for CTCI x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card:

- Sets the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Sets the Online Requested by Card Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.8 Velocity Checking for Consecutive International Country Transactions Lower Limit

This optional card check generates a request for an online authorization if the limit on the number of international offline transactions since the counter was reset 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.

Note: *When Profiles Functionality is supported, the counter may be checked against the limit regardless of the country in which the transaction takes place.*

When Profiles Functionality is not supported, the counter is checked against the limit only for an international country transaction.

If Profiles Functionality is not supported, and the Issuer Country Code, Consecutive Transaction Counter International Country (CTCIC), and Consecutive Transaction Counter International Country Limit (CTCICL) are present; then the card shall perform the following check:

- The card shall check whether the sum of the CTCIC plus one is greater than the CTCICL if *both* of the following are true:
  - the Terminal Country Code isnot equal to the Issuer Country Code
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC) or online authorization (ARQC)

  Otherwise, if the Terminal Country Code is not equal to the Issuer Country Code; then the card checks whether the CTCIC is greater than the CTCICL.

If Profiles Functionality is supported, and the Issuer Country Code, Consecutive Transaction Counter International Country x, and Consecutive Transaction Counter International Country Limit x are present; then the card shall perform the following check for each Consecutive Transaction Counter International Country x:

- The card shall check whether the sum of the Consecutive Transaction Counter International Country x plus one is greater than the Consecutive Transaction Counter International Country Limit x if *all* of the following are true:
  - the 'Allow Counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b
  - the Terminal Country Code is not equal to the Issuer Country Code
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC) or online authorization (ARQC)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Otherwise, the card shall check whether the Consecutive Transaction Counter International Country x is greater than the Consecutive Transaction Counter International Country Limit x if *either* of the following is true:

– the 'Allow Counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b

– the 'Check limits for CTCIC x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card:

- Sets the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Sets the Online Requested by Card Indicator to 1b.

11.4.3.9 Velocity Checking for Cumulative Total Transaction Amount Lower Limit

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 designated application currency (and in alternate designated currencies if currency conversion is supported) has been exceeded.

Note: *When Profiles Functionality is supported, the amount may be checked against the limit regardless of the transaction currency.*

When Profiles Functionality is not supported, the amount is checked against the limit only if the transaction is in the application currency or in a currency that can be approximately converted.

When processing the transaction, if *all* of the following are true:

- currency conversion is supported (that is, the application is capable of currency conversion, and the Currency Conversion Parameters data element is present)
- the Transaction Currency Code does not equal the Application Currency Code
- the Transaction Currency Code equals one of the Conversion Currency Codes in the Currency Conversion Parameters

then the Amount, Authorized and the Currency Conversion Factor x associated with the matching Conversion Currency Code x (the values of "x" are the same) are used to calculate the approximate value of the transaction in the application currency.

Otherwise, the Transaction Currency Code does not equal any of the Conversion Currency Codes in the Currency Conversion Parameters.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If Profiles Functionality is not supported and the Application Currency Code, Cumulative Total Transaction Amount (CTTA), and Cumulative Total Transaction Amount Limit (CTTAL) are present, then the card shall perform the following check:

- If the Transaction Currency Code equals the Application Currency Code, then the card checks whether the the sum of the Cumulative Total Transaction Amount and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Limit,

  Otherwise, if the Transaction Currency Code equals one of the Conversion Currency Codes in the Currency Conversion Parameters, then the card checks whether the sum of the Cumulative Total Transaction Amount and the approximate value of the transaction in the application currency is greater than the Cumulative Total Transaction Amount Limit.

If Profiles Functionality is supported and the Application Currency Code, Cumulative Total Transaction Amount x and Cumulative Total Transaction Amount Limit x are present; then the card shall perform the following check for each Cumulative Total Transaction Amount x:

- The card checks whether the sum of the Cumulative Total Transaction Amount x and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Limit x if *both* of the following are true:
  - the ‘Allow Counting in CTTA x’ bit of the Profile Control for the transaction is set to 1b;
  - the Transaction Currency Code equals the Application Currency Code

  Otherwise the card shall check whether the sum of the Cumulative Total Transaction Amount x and the approximate value of the transaction in the application currency is greater than the Cumulative Total Transaction Amount Limit x if *both* of the following are true:
  - the ‘Allow Counting in CTTA x’ bit of the Profile Control for the transaction is set to 1b
  - the Transaction Currency Code equals one of the Conversion Currency Codes in the Currency Conversion Parameters

  Otherwise, the card shall check whether the Cumulative Total Transaction Amount x is greater than the Cumulative Total Transaction Amount Limit x if *either* of the following is true:
  - the ‘Allow Counting in CTTA x’ bit of the Profile Control for the transaction is set to 1b
  - the ‘Check limits for CTTA x’ bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Sets the ‘Exceeded velocity checking counters’ bit of the CVR to 1b.
- Sets the Online Requested by Card Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

EXAMPLE: CONVERTING BRITISH POUNDS TO EUROS

- The designated Application Currency is the Euro.
- The Conversion Currency 1 is the Pound.
- Conversion rate is 1.36 Euros per Pound.
- Currency Conversion Factor 1 is 10000014:
  - The first nibble indicates that the decimal point is one digit from the right.
  - The last seven nibbles of 0000014 represent 1.36 reduced to two significant digits.
- Amount Authorized is 150.00 Pounds
  (15000 with an implied two decimal places).
- Cumulative Total Transaction Amount (CTTA) prior to transaction is 80000 (800.00 Euros)
- Cumulative Total Transaction Amount Limit (CTTAL) is 100000 (1000.00 Euros).

1. Multiply (Amount Authorized in Pounds) by
   (Currency Conversion Factor 1 without first nibble).

   15000 x 14 = 210000

2. Shift decimal point by the first nibble of Currency Conversion Factor 1

   first nibble = 1, so:

   210000 $\rightarrow$ 21000 (210.00 Euros)

3. Compare (result plus Cumulative Total Transaction Amount) to Cumulative Total Transaction AmountLimit.

   ((21000 + 80000) $\leq$ 100000) = FALSE

   The limit is exceeded.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.10 Velocity Checking for Contactless Offline Transactions Lower Limit

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

The card shall perform this check if the card supports offline contactless functionality (such as qVSDC); and the Contactless Transaction Counter (CLTC), and the Contactless Transaction Counter Lower Limit (CLTCLL) are present; and if Profiles Functionality is supported, the 'Check limits for CLTC' bit of the Profile Control for the transaction is set to 1b.

If the CLTC is greater than or equal to the CLTCLL, then the card shall:

- Set the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Set the Online Requested by Card Indicator to 1b.

11.4.3.11 Velocity Checking for VLP Contactless Transactions Reset Threshold

This optional card check generates a request for an online authorization if the limit on the amount of offline contactless transactions in the VLP Available Funds has been exceeded.

The card shall perform this check if all of the following are true:

- the card supports offline contactless functionality (such as qVSDC)
- the VLP Available Funds, and VLP Reset Threshold are present
- if Profiles Functionality is supported, the 'Check limits for VLP Available Funds' bit of the Profile Control for the transaction is set to 1b.

If the VLP Available Funds is less than or equal to the VLP Reset Threshold, then the card shall:

- Set the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Set the Online Requested by Card Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.12New 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, then the card:

- Sets the ‘New card’ bit of the CVR to 1b.
- Sets the Online Requested by Card Indicator to 1b if either of the following is true:
  - Profiles Functionality is not supported and the ‘If new card, transmit transaction online’ bit of the ADA is set to 1b,
  - Profiles Functionality is supported and the ‘If new card, transmit transaction online’ bit of the Profile Control chosen for the transaction is set to 1b

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.13Offline 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, then 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

then the card shall perform the following actions:

- Set the 'PIN Try Limit exceeded' bit of the CVR to 1b.
- If the 'If PIN Try Limit exceeded on previous transaction, decline transaction' bit of the ADA equals 1b, set Offline Decline Requested by Card Indicator to 1b.
- Set Online Requested by Card Indicator to 1b if either of the following is true:
  - Profiles Functionality is not supported and the 'If PIN Try Limit exceeded on previous transaction, transmit transaction online' bit of the ADA equals 1b.
  - Profiles Functionality is supported and the 'If PIN Try Limit exceeded on previous transaction, transmit transaction online' bit of the Profile Control chosen for the transaction equals 1b.
- If the 'If PIN Try Limit exceeded on previous transaction, decline and block application' bit of the ADA equals 1b, decline the transaction and block the application.

11.4.3.14Go Online on Next Transaction From Previous Online Response

This conditional check is required if CVN 18 and Issuer Authentication are supported. It determines whether during a previous transaction where Issuer Authentication was successful, the issuer wanted the card to go online for subsequent transactions. The issuer indicated this by setting the 'Set Go Online on Next Transaction' bit in the verified Card Status Updates (CSU) of a previous transaction to 1b, causing the Go Online on Next Transaction Indicator to be set to 1b.

If the indicator is set, then the card requests online processing until the indicator is reset.

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

If the Go Online on Next Transaction Indicator is set to 1b, then the card shall set the Online Requested by Card Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.4.3.15Special Transactions

This check was deleted in VIS 1.5.3.

11.4.3.16PIN Verification Not Performed or Not Successful for a PIN-Expecting Card

This optional check for cards supporting Offline PIN verification generates a request for an online authorization if the issuer wanted the card to go online for authorization when Offline (plaintext or enciphered) PIN was not performed or was not successful.

If this check is to be performed, then if *both* of the following are true:

- the 'Offline PIN verification performed' bit of the CVR equals 0b or the 'Offline PIN verification failed' bit of the CVR equals 1b
- *and* the 'If Offline PIN verification not performed or not successful, send transaction online' bit of the ADA equals 1b

the card shall set the Online Requested by Card Indicator to 1b.

11.4.3.17VERIFY Not Received by PIN-Expecting Card

This optional check for cards supporting Offline PIN verification sets an indicator if the application prefers Offline (plaintext or enciphered) PIN to be performed but no VERIFY command is received by the card.

If this check is to be performed, then if the 'Offline PIN verification performed' bit of the CVR is 0b *and* the 'If Offline PIN verification not performed or not successful, send transaction online' bit of the ADA is 1b, the card shall set the 'PIN verification command not received for a PIN-Expecting card' bit of the CVR to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 1b. The card's decision to go online is indicated by the Online Requested by Card Indicator equal to 1b.

An online-only card shall not respond to the first GENERATE AC command with a TC. If the transaction is not declined (that is, the terminal did not request an AAC and the Offline Decline Requested by Card Indicator has the value 0b), then the card shall respond with an ARQC to request that the transaction go online.

The card sets the CVR and CID 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.

If the application supports IAD Format 2, and the 'CDCVM Supported' bit of the ADA is set to 1b, then the application shall set the 'CDCVM Successfully Performed' bit of the CVR to 1b.

Note: *This bit will always be set in the CVR for IAD Format 2 if the ADA indicates that CDCVM is supported.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

If the application supports Issuer Scripts and IAD Format 2, then set the 'Secure Messaging uses EMV Session key-based derivation' bit of the CVR to the value of the 'Secure Messaging uses EMV Session key-based derivation' bit in the ADA.

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 building the Issuer Application Data and generating the Application Cryptogram to send in the response, the card shall increment counters, if present, as follows:

- If Profiles Functionality is not supported:
  - If the Terminal Country Code is not equal to the Issuer Country Code, and the 'Do not count declined transactions' bit of the ADA is set to 0b, then increment the Consecutive Transaction Counter International Country (CTCIC) by one.
  - Increment the Consecutive Transaction Counter International (CTCI) by one if the 'Do not count declined transactions' bit of the ADA is set to 0b *and either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
    - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
  - If the 'Do not count declined transactions' bit of the ADA is set to 0b, then increment the Consecutive Transaction Counter (CTC) by one.
- If Profiles Functionality is supported:
  - increment each Consecutive Transaction Counter International Country x by one if *all* of the following are true:
    - the Terminal Country Code is not equal to the Issuer Country Code
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the 'Allow counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- increment each Consecutive Transaction Counter International x (CTCI x) by one if *all* of the following are true:
  - *either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code *nor* to any of the Conversion Currency Codes in Currency Conversion Parameters
    - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
  - the 'Do not count declined transactions' bit of the ADA is set to 0b
  - the 'Allow counting in CTCI x' bit of the Profile Control for the transaction is set to 1b
- increment each Consecutive Transaction Counter x if *both* of the following are true:
  - the 'Do not count declined transactions' bit of the ADA is set to 0b
  - the 'Allow counting in CTC x' bit of the Profile Control for the transaction is set to 1b

If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then after updating counters, but prior to generating the AAC, the Issuer Discretionary Data portion of the Issuer Application Data shall be built as described in Appendix J.

Prior to responding, the card shall:

1. Check the Application Default Action (ADA):
   - If the 'If transaction declined offline, create advice' bit of the ADA is set to 1b, then set the 'Advice required' bit of the Cryptogram Information Data (CID) to 1b
   - If PIN Try Limit has been exceeded on this transaction and the ADA indicates that an advice is required when this occurs, then:
     - Set the 'Advice required' bit of the CID to 1b
     - If the 'Reason/Advice Code' of the CID is not set to 'Service not allowed', then set it to 'PIN Try Limit exceeded'

       Note: *The 'Service not allowed' value in the CID takes precedence over all other reason codes.*
2. Check the TVR provided by the terminal in the GENERATE AC command:
   - If the 'SDA failed' bit of the TVR is set to 1b, then set the Static Data Authentication Failure Indicator to 1b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– If the ‘DDA failed’ bit or the ‘CDA failed’ bit of the TVR is set to 1b, then set the Dynamic Data Authentication Failure Indicator to 1b

Counter increments have been moved - they now occur prior to building the Issuer Application Data.

3. If all of the following are true, then log the transaction:
   – Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
   – The ‘Include declined transactions in the transaction log’ bit of the ADA is set to 1b.
   – If Profiles Functionality is supported, the ‘Log transactions performed using this profile’ bit of the Profile Control chosen for the transaction is set to 1b.
   – If transaction logging is limited by Transaction Type; the Transaction Type is set to '00' (Purchase), '01' (Cash), or '11' (Quasi cash).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then prior to generating the ARQC, the Issuer Discretionary Data portion of the Issuer Application Data is built as described in Appendix J.

Prior to responding, the card sets the Online Authorization Indicator to 1b.

The response includes the CID, ATC, ARQC type Application Cryptogram, and Issuer Application Data.

Note: *The following counters are **not** incremented at this time:*

Consecutive Transaction Counter (CTC)
Consecutive Transaction Counter International (CTCI)
Consecutive Transaction Counter International Country (CTCIC)
Cumulative Total Transaction Amount
Contactless Transaction Counter (CLTC)
Any Consecutive Transaction Counter x (CTC x)
Any Consecutive Transaction Counter International x (CTCI x)
Any Consecutive Transaction Counter International Country x (CTCIC x)
Any Cumulative Total Transaction Amount x

Also, VLP Available Funds is not decremented at this time.

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 building the Issuer Application Data and generating the TC to send in the response, the card shall update counters, if present, as follows:

- If Profiles Functionality is not supported, the card updates counters as follows:
  - Increment the Consecutive Transaction Counter (CTC) by one.
  - If the Terminal Country Code is not equal to the Issuer Country Code, then increment the Consecutive Transaction Counter International Country (CTCIC) by one.
  - If the Transaction Currency Code is equal to the Application Currency Code, then increment the Cumulative Total Transaction Amount by the Amount, Authorized.
  - Increment the Consecutive Transaction Counter International (CTCI) by one if *either* of the following is true:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
- the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b

– If the Transaction Currency Code is not equal to the Application Currency Code but is equal to one of the Conversion Currency Codes in Currency Conversion Parameters, then increment the Cumulative Total Transaction Amount by the approximate value of the amount converted to the Application Currency (using the Amount, Authorized and the Currency Conversion Factor associated with the matching Conversion Currency Code).

- If Profiles Functionality is supported, the card updates counters, if present, as follows:
  – For each Consecutive Transaction Counter x; if the 'Allow counting in CTC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter x by one
  – If the Terminal Country Code is not equal to the Issuer Country Code; then for each Consecutive Transaction Counter International Country x, if the 'Allow counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b, increment the Consecutive Transaction Counter International Country x by one
  – For each Cumulative Total Transaction Amount x, if the 'Allow counting in CTTA x' bit of the Profile Control for the transaction is set to 1b:
    - if the Transaction Currency Code is equal to the Application Currency Code, then increment the Cumulative Total Transaction Amount x by the Amount, Authorized.
    - If the Transaction Currency Code is not equal to the Application Currency Code but is equal to one of the Conversion Currency Codes in Currency Conversion Parameters, then increment the Cumulative Total Transaction Amount x by the approximate value of the amount converted to the Application Currency (using the Amount, Authorized and the Currency Conversion Factor associated with the matching Conversion Currency Code).
  – for each Consecutive Transaction Counter International x (CTCI x), if the 'Allow counting in CTCI x' bit of the Profile Control for the transaction is set to 1b, increment the Consecutive Transaction Counter International x by one if *either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- the Terminal Country Code does not match the Issuer Country Code and the ‘CTCI also counts non-matching country code transactions’ bit of the ADA is set to 1b.

- If the card supports qVSDC functionality, and all the following conditions are true, then reset the VLP Available Funds to the VLP Funds Limit used for qVSDC functionality:
  - the offline PIN was successfully verified (that is, the ‘Offline PIN verification performed’ bit in the CVR is set to 1b and the ‘Offline PIN verification failed’ bit in the CVR is set to 0b)
  - the ‘Low-value AND CTTA Check Supported’ bit in the Card Additional Processes is set to 1b
  - the ‘Reset VLP Available Funds to VLP Funds Limit whenever Offline PIN is successfully verified’ bit in the ADA is set to 1b
  - the card is not a new card (that is, the Last Online ATC is not zero)
  - if Profiles Functionality is supported, the ‘Allow reset of VLP Available Funds’ bit of the Profile Control for the transaction is set to 1b

If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then after updating counters, but prior to generating the TC, the Issuer Discretionary Data portion of the Issuer Application Data shall be built as described in Appendix J.

Prior to responding:

- If all of the following are true, then the card logs the transaction:
  - Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
  - The ‘Do not include offline approved transactions in the transaction log’ bit of the ADA is set to 0b.
  - If Profiles Functionality is supported, the ‘Log transactions performed using this profile’ bit of the Profile Control chosen for the transaction is set to 1b.
  - If transaction logging is limited by Transaction Type; the Transaction Type is '00' (Purchase), '01' (Cash), or '11' (Quasi cash).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.5.4 CDA Requested

The terminal requests CDA when the “CDA Signature Requested” bit of the GENERATE AC command's P1 parameter is set to 1b.

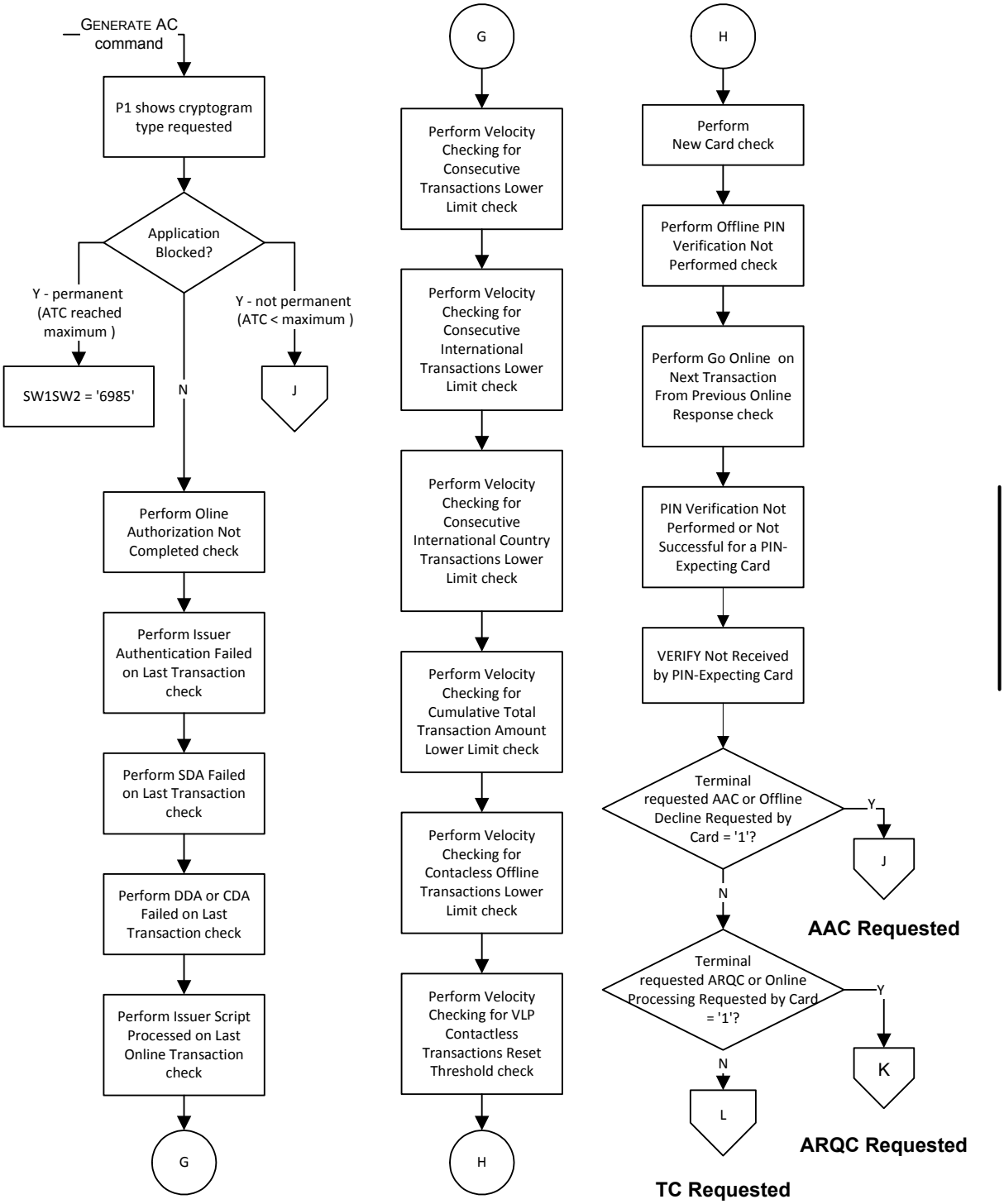
Upon determining that the terminal is requesting CDA, the card shall:

1. Perform standard Card Risk Management and determine the type of Application Cryptogram (AAC, TC, or ARQC) that will be sent in the GENERATE AC response.
2. If the card’s response is an AAC, then generate the Application Cryptogram as described above and return the AAC in the GENERATE AC response as shown in *EMV Book 3*, Table 13.
3. If the card’s response is an ARQC or TC, then return the Application Cryptogram in an RSA envelope as follows:
   a. Prior to generating the Application Cryptogram, set the ‘Offline dynamic data authentication performed’ bit of the CVR to 1b.
   b. Generate the TC or ARQC Application Cryptogram as described above.
   c. Return the Application Cryptogram in an RSA envelope as follows:
      i. Generate a dynamic signature from the Application Cryptogram as described in *EMV Book 2*, section 6.6.1, and summarized in the bullets below:
         – Apply the SHA-1 algorithm to a concatenation of the following data to form the Transaction Data Hash Code
            • The values in the data elements sent by the terminal in the GET PROCESSING OPTIONS command
            • The values sent by the terminal in the first GENERATE AC command
            • The tags, lengths, and values of the data elements to be returned by the ICC in the response to the first GENERATE AC command in the order they are returned, with the exception of the Signed Dynamic Application Data.
         – Concatenate the data indicated in *EMV Book 2*, Table 17. This data includes the ICC Dynamic Data which (as shown in *EMV Book 2*, Table 18) contains the ICC Dynamic Number Length, ICC Dynamic Number, Cryptogram Information Data, Application Cryptogram (TC or ARQC), and Transaction Data Hash Code.
         – Generate a hash value from the concatenated data.
         – Include the hash in the Signed Dynamic Application Data.
         – Sign the Signed Dynamic Application Data with the ICC Private Key.
      ii. Include the signature of the Signed Dynamic Application Data in the GENERATE AC response.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

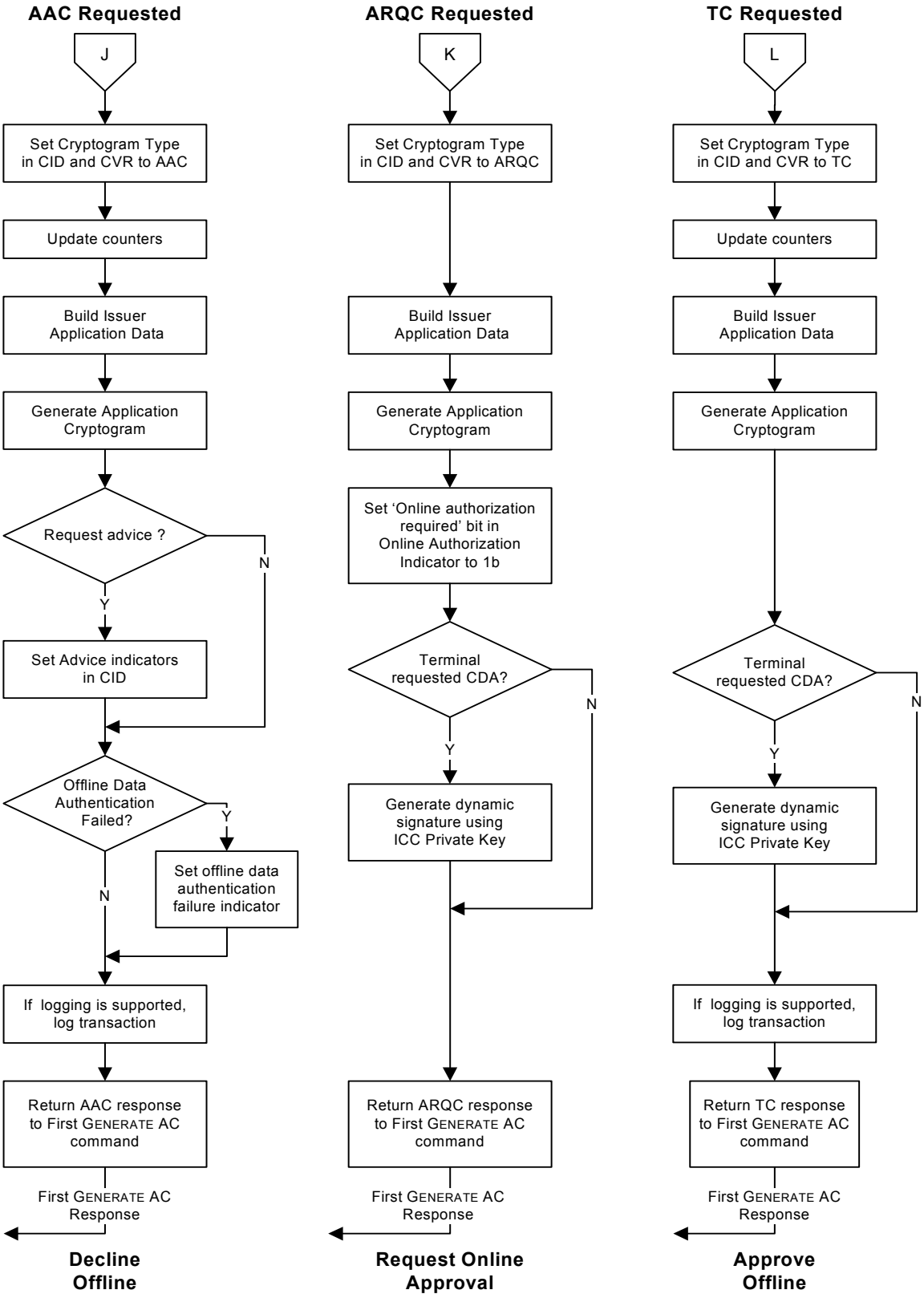
11.6 Processing Flow

Figure 11-1: Card Action Analysis Processing Flow (1 of 2)



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

11.7 Prior Related Processing

Initiate Application Processing

If the Profiles Functionality is supported, Profile Selection determines the Profile ID that identifies which Profile Control x to use for customizing processing of the transaction for the specific transaction environment.

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, then 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

12 Online Processing

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/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 *EMV Book 3*, section 10.9, and *EMV Book 4*, section 6.3.8.

This chapter includes the following 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

12.1 Card Data

The terminal uses the data from the card, described in Table 12-1, during processing of the online request or during the Issuer Authentication portion of Online Processing. For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

Table 12-1: Online Processing, Issuer Authentication—Card Data (1 of 2)

Data Element	Description
Application Cryptogram, '9F26'	The online cryptogram (ARQC) value from the card. Received from the card in the GENERATE AC response.
Application Interchange Profile (AIP), '82'	The AIP was sent to the terminal by the card during Initiate Application Processing. The 'Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command' bit of the AIP shall be set to: • 1b if the card supports Issuer Authentication using the EXTERNAL AUTHENTICATE command (for example, for CVN 10). • 0b if the card either supports Issuer Authentication as part of processing the GENERATE AC command (for example, for either CVN 10 or CVN 18), or does not support Issuer Authentication. ***Note:*** *Issuer authentication for CVN 18 is only to be performed as part of second GENERATE AC command processing, so the AIP for a card using CVN 18 shall not indicate that Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command.*
Application Transaction Counter (ATC), '9F36'	Counter of transactions initiated with the card application since the application was put on the card. Received from the card in the GENERATE AC response.
Authorization Request Cryptogram (ARQC)	The cryptogram calculated by the card during Card Action Analysis that is input to the Authorization Response Cryptogram (ARPC) validation. Used during Issuer Authentication portion of Online Processing.
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. Used during Issuer Authentication portion of Online Processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 12-1: Online Processing, Issuer Authentication—Card Data (2 of 2)

Data Element	Description
Cryptogram Information Data (CID), '9F27'	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 10b in the first two bits (bits 8–7) of this field. Received from the card in the GENERATE AC response.
Issuer Application Data, '9F10'	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, VIS Data Element Tables. For Cryptogram Version Numbers 10 and 18 (CVN 10 and CVN 18), 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. Received from the card in the GENERATE AC response.
Issuer Authentication Failure Indicator	The card sets the Issuer Authentication Failure Indicator to 1b if Issuer Authentication fails. Used during Issuer Authentication portion of Online Processing.
Issuer Authentication Performed Using EXTERNAL AUTHENTICATE Command Indicator	Indicates whether Issuer Authentication was already performed during the current transaction using the EXTERNAL AUTHENTICATE command. This indicator is set during Issuer Authentication portion of Online Processing and is used during Completion processing to ensure the application does not perform Issuer Authentication again for the same transaction as part of processing the second GENERATE AC command.
Unique DEA Key A and B (UDKs)	The card's secret DES keys which the card uses to validate the ARPC. Used during Issuer Authentication portion of Online Processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

12.2 Online Response Data

The online response from the issuer to the terminal contains the data described in Table 12-2. If the card is to perform Issuer Authentication using the EXTERNAL AUTHENTICATE command, 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 12-2: Online Processing, Issuer Authentication—Terminal Data

Data Element	Description
Issuer Authentication Data (IAuD), '91'	Data that the terminal includes in either the EXTERNAL AUTHENTICATE command or the GENERATE AC command sent to the card. The contents of the Issuer Authentication Data depends on the Cryptogram Version Number. For CVN 10, the application uses the following data elements contained within the Issuer Authentication Data: • Authorization Response Cryptogram (ARPC) — An 8-byte cryptogram generated by the issuer host (or its agent) and passed to the terminal in the online response. • ARPC Response Code —The 2-byte response code indicating the issuer's decision regarding the outcome of the online authorization. It is used in the calculation of the ARPC and passed to the terminal in the online response from the issuer. Other Visa documentation also refers to this data element as the Authorization Response Code. *Optional issuer data is not supported for CVN 10.* For CVN 18, the application uses the following data elements contained within the Issuer Authentication Data: • Authorization Response Cryptogram (ARPC)— A 4-byte cryptogram generated by the issuer host (or its agent) and passed to the terminal in the online response. • Card Status Update (CSU) — A 4-byte data element that indicates whether the issuer approves or declines the transaction, and indicators used to initiate actions specified by the issuer to update the card or application. • Proprietary Authentication Data — An optional 1 to 8-byte data element containing additional data from the issuer sent in the online response and validated during Issuer Authentication. The use of this additional data is beyond the scope of this specification.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

12.3 EXTERNAL AUTHENTICATE Command

The EXTERNAL AUTHENTICATE command is sent to the card by the terminal when Issuer Authentication should be performed using this command instead of as part of second GENERATE AC command processing. This command shall be performed as described in *EMV Book 3*, section 6.5.4 and section D.3.3, Generating the Authorization Response Cryptogram (ARPC) for CVN 10 ('0A'), in this document.

If the application generates the Application Cryptogram using a CVN that only supports Issuer Authentication during the second GENERATE AC command (e.g., CVN 18 or CVN '22'), then the AIP must not be configured to request that the terminal perform Issuer Authentication using the EXTERNAL AUTHENTICATE command. If the application supports the EXTERNAL AUTHENTICATE command, and erroneously receives the command for a cryptogram version that only supports Issuer Authentication during second GENERATE AC, the application does not perform Issuer Authentication during EXTERNAL AUTHENTICATE command processing, and responds to the terminal with SW1 SW2 = '6983'. The card performs Issuer Authentication later during the second GENERATE AC command processing, as specified in section 13.6, and sets the CVR bits accordingly.

Note: *Issuers of cards that perform Issuer Authentication during second GENERATE AC command processing (instead of EXTERNAL AUTHENTICATE) must evaluate the indicators in the CVR (instead of the TVR) to determine the result of Issuer Authentication.*

If the AIP indicates that Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command, then 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

12.4.3 Issuer Authentication using the EXTERNAL AUTHENTICATE command

The terminal sends an EXTERNAL AUTHENTICATE command to the card if the Application Interchange Profile (AIP) from the card indicates Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command 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 (that is, the Issuer Authentication Was Performed Using the EXTERNAL AUTHENTICATE Command Indicator has the value 1b):
   - Set Issuer Authentication Failure Indicator to '1'.
   - Respond to terminal with SW1 SW2 = '6985'.
2. if the application generates the Application Cryptogram using a CVN that only supports Issuer Authentication during the second Generate AC command (e.g., CVN 18 or CVN '22'), then the application shall:
   - Respond to the terminal with SW1 SW2 = '6983'
   - Not perform Issuer Authentication in the EXTERNAL AUTHENTICATE command
   - Not change the setting of:
     - the Issuer Authentication Failure Indicator
     - the 'Issuer Authentication performed and failed' bit of the CVR
     - the Issuer Authentication Was Performed using the EXTERNAL AUTHENTICATE Command Indicator

   Otherwise, parse out the ARPC Response Code included in the Issuer Authentication Data for CVN 10 and store it for later use during the Completion processing function.

   Note: *CVN 10 is the only VIS-defined cryptogram that is supports Issuer Authentication using the EXTERNAL AUTHENTICATE command.*

   For proprietary cryptograms , the process for determing whether Issuer Authentication passed or failed is outside the scope of this specification, but after determining the Issuer Authentication result, processing should continue as described in step 5.
3. Generate an Authorization Response Cryptogram (ARPC) from the ARPC Response Code and the ARQC returned with the first GENERATE AC response using the algorithm described in Appendix D, Authentication Data, Keys and Algorithms, and the Unique DEA Keys (UDKs) stored in the card for the application.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

4. Compare the generated ARPC to the ARPC received in the EXTERNAL AUTHENTICATE command. If they are the same, then Issuer Authentication is considered successful. If they are different, then Issuer Authentication is considered failed.
5. If Issuer Authentication is successful, then the card shall:
   a. Set the Issuer Authentication Failure Indicator to 0b.
   b. If the card supports contactless issuer update processing, set the Last Successful Issuer Update ATC Register to the value of the ATC.
   c. Set the Issuer Authentication Was Performed Using the EXTERNAL AUTHENTICATE Command Indicator to 1b.
   d. Use the ARPC Response Code that was verified by Issuer Authentication passing when processing the transaction as described in section 13.7.
   e. Indicate that Issuer Authentication was successful in the EXTERNAL AUTHENTICATE command response sent to the terminal (SW1 SW2 = '9000').

If Issuer Authentication fails, then the card shall:

a. Set the Issuer Authentication Failure Indicator to 1b.
b. Set the ‘Issuer Authentication performed and failed’ bit of the CVR to 1b.
c. Set the Issuer Authentication Was Performed Using the EXTERNAL AUTHENTICATE Command Indicator to 1b.
d. Not use the ARPC Response Code received from the terminal when processing the transaction as described in section 13.7.
e. 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 1b 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 whether that transaction should be transmitted online.

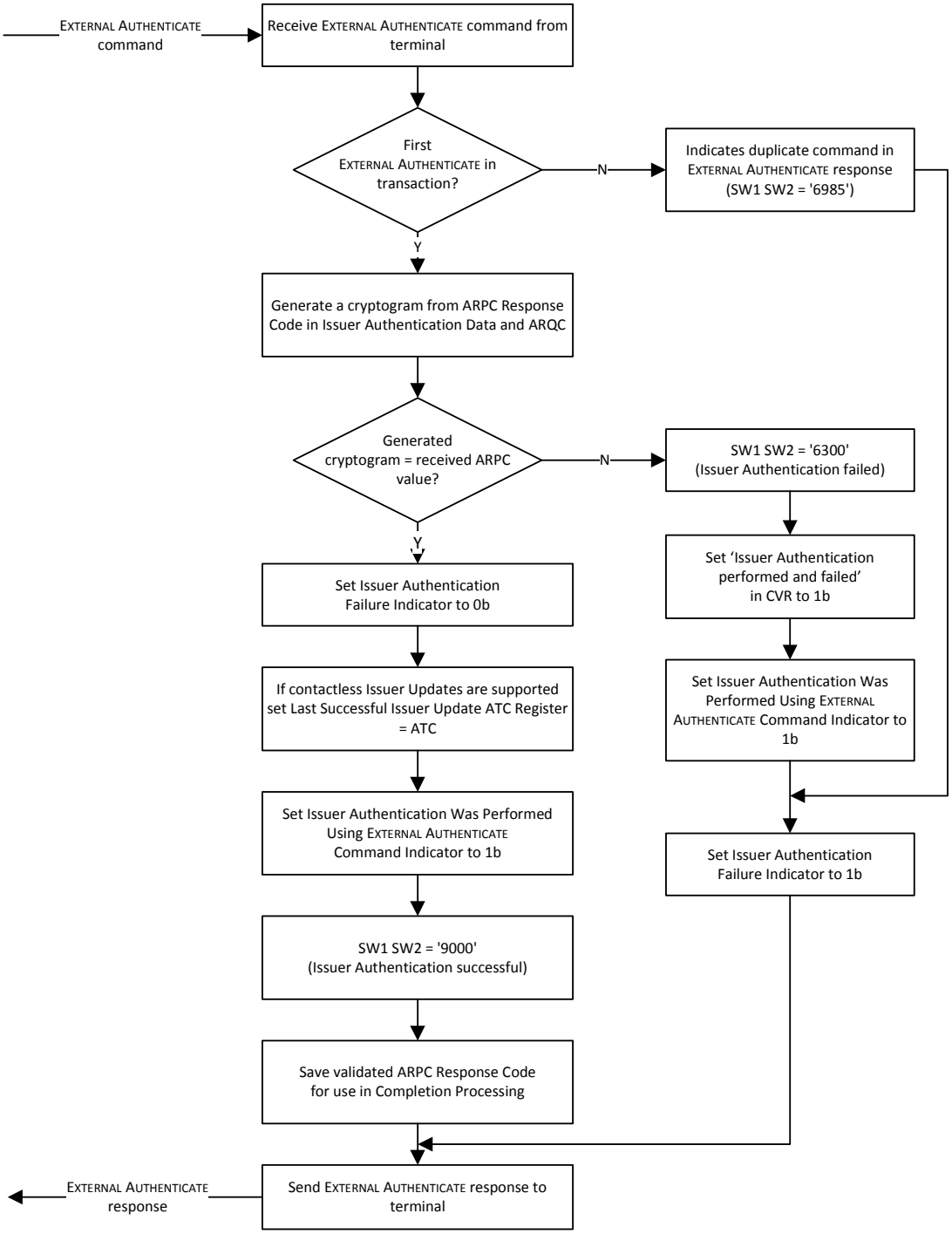
During Completion processing, the card shall be able to determine whether Issuer Authentication was performed and successful for the transaction since the response to the final GENERATE APPLICATION CRYPTOGRAM may be dependent upon these results.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

12.5 Processing Flow

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

Figure 12-1: Online Processing Flow



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 using the EXTERNAL AUTHENTICATE command.

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 does not consider Issuer Authentication results (from the EXTERNAL AUTHENTICATE command or from the GENERATE AC command) when 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, then the card will send the transaction online for an authorization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13 Completion Processing

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, then 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 *EMV Book 3*, section 10.11, and *EMV Book 4*, section 12.2.1.

This chapter includes the following sections:

13.1 Card Data
13.2 Terminal Data
13.3 GENERATE APPLICATION CRYPTOGRAM (AC) Command
13.4 Completion Processing Overview and Flow
13.5 Receive GENERATE AC Command
13.6 Processing Response Data for Online Authorized Transaction
13.7 Complete Response for Online Authorized Transaction
13.8 Online Processing Requested, Online Authorization Not Completed
13.9 CDA Requested
13.10 Prior Related Processing
13.11 Subsequent Related Processing

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.1 Card Data

The card uses the card data described in Table 13-1 during Completion either internally, to request data from the terminal for use in Completion processing, or in generating the GENERATE AC response which the card returns to the terminal. For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables. For an overview of the types of counters and the related limits used in VIS, please see Appendix G, Overview of Velocity-Checking Counters.

Table 13-1: Completion—Card Data (1 of 8)

Data Element	Description
Application Capabilities, 'DF01' in 'BF5B'	Indicates card application capabilities such as contactless enabled or disabled.
Application Cryptogram (AC), '9F26'	The value of the cryptogram. If the transaction was eligible for CDA and the Cryptogram Information Data shows that the cryptogram is an ARQC or TC, then the Application Cryptogram and other data are enclosed within an RSA signature. Sent to the issuer in the GENERATE AC response.
Application Currency Code, '9F51'	Indicates the currency in which the account is managed.
Application Default Action (ADA), '9F52'	A Visa proprietary data element indicating the issuer-specified action a card should take when exception conditions occur.
Application Interchange Profile (AIP), '82'	Indicates ability of the card to support specific functions including Issuer Authentication using the EXTERNAL AUTHENTICATE command.
Application Transaction Counter (ATC), '9F36'	A counter of the number of transactions initiated since the application was put on the card. Sent to the issuer in the GENERATE AC response.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (2 of 8)

Data Element	Description
Card Risk Management Data Object List 2 (CDOL2), '8D'	A list of tags and lengths of the terminal data elements that the terminal should include in the second GENERATE AC command. The tags and lengths of the following data elements shall be included in CDOL2 if the Application Cryptogram is generated using Cryptogram Version Number 10 or 18 (CVN 10 or CVN 18), because the value is input to the cryptogram and may be different from the value used in processing the first GENERATE AC command: • Amount, Authorized • Amount, Other • Terminal Verification Results (TVR) • Unpredictable Number The tags and lengths of the following data elements should be included in CDOL2 if the Application Cryptogram is generated using CVN 10 or CVN 18, unless the data element value is saved from processing the first GENERATE AC command: • Terminal Country Code • Transaction Currency Code • Transaction Date • Transaction Type The tag and length of the Issuer Authentication Data data element shall be included in CDOL2 if Issuer Authentication is supported (the Issuer Authentication Indicator is present) and the AIP indicates that Issuer Authentication is not supported using the EXTERNAL AUTHENTICATE command, because the data is needed to perform Issuer Authentication. If not already included in CDOL2 for cryptogram generation, the tags and lengths of the following data elements shall also be included in 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 are supported) • Terminal Country Code (if checks requiring country code are supported) • Any data elements needed for logging transactions internal to the card during second GENERATE AC processing, unless the data element value is saved from processing the first GENERATE AC command. Tags and lengths for any of the data elements that are already included in CDOL2 as part of the terminal data used for cryptogram generation should not be repeated in CDOL2 for use in other Completion functions.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (3 of 8)

Data Element	Description
Consecutive Transaction Counter (CTC), 'DF11' in'BF56'	A Visa proprietary counter that is incremented for each offline approved (and optionally for each declined) transaction. This counter may be reset or updated during Completion Processing.
Consecutive Transaction Counter Upper Limit (CTCUL), '9F59', or 'DF31' in 'BF56'	A Visa proprietary data element indicating the maximum number of consecutive offline transactions that can be conducted before a transaction will be declined offline if it cannot be sent online. *Renamed from: Upper Consecutive Offline Limit ('9F59')*
Consecutive Transaction Counter International (CTCI), 'DF11' in 'BF57'	A Visa proprietary counter that is incremented for each offline approved (and optionally for declined) transaction which is either not in the card's designated currency and if currency conversion is supported is also not in a designated alternate currency, or optionally is not in the issuers country. This counter may be reset or updated during Completion Processing.
Consecutive Transaction Counter International Country (CTCIC), 'DF51' in 'BF57'	Visa proprietary counter that is incremented for each offline approved (and optionally for declined) transaction where the Issuer Country Code differs from the Terminal Country Code. This counter may be reset or updated during Completion Processing.
Consecutive Transaction International Upper Limit (CTIUL), '9F5E', or 'DF31' in 'BF57'	A Visa proprietary data element indicating the maximum number of offline international (based on country or currency) transactions since the counter was reset. The same limit is used to limit international country transactions and international currency transactions.
Consecutive Transaction Counter x (CTC x), 'DF1x' in 'BF56' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTC x: CTC 1, CTC 2, CTC 3, CTC 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTC x in the Profile.
Consecutive Transaction Counter Upper Limit x (CTCUL x), 'DF3x' in 'BF56' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCUL x: CTCUL 1, CTCUL 2, CTCUL 3, CTCUL 4. Each CTCUL x is used as the upper limit for the corresponding CTC x.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (4 of 8)

Data Element	Description
Consecutive Transaction Counter International x (CTCI x), 'DF1x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCI x: CTCI 1, CTCI 2, CTCI 3, CTCI 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTCI x in the Profile.
Consecutive Transaction Counter International Country x (CTCIC x), 'DF5x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTCIC x: CTCIC 1, CTCIC 2, CTCIC 3, CTCIC 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTCIC x in the Profile.
Consecutive Transaction International Upper Limit x (CTIUL x), 'DF3x' in 'BF57' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTIUL x: CTIUL 1, CTIUL 2, CTIUL 3, CTIUL 4. Each CTIUL x is used as the upper limit for the corresponding CTCI x and CTCIC x.
Contactless Transaction Counter (CLTC), 'DF11' in 'BF55'	A Visa proprietary counter that is incremented for each offline contactless domestic transaction.
Contactless Transaction Counter Upper Limit (CLTCUL), 'DF31' in 'BF55'	The number of offline contactless domestic transactions allowed before online processing is requested.
Conversion Currency Code x *for minimum implementations of currency conversion, x = 1 to 5*	A code identifying an alternate currency to be converted to the Application Currency for multiple currency velocity checking.
Cryptogram Information Data (CID), '9F27'	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 Sent to the terminal in the GENERATE AC response.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (5 of 8)

Data Element	Description
Cumulative Total Transaction Amount (CTTA), 'DF11' in 'BF58'	A Visa proprietary data element specifying the total accumulated amount for offline approved transactions in the designated currency (Application Currency Code) plus the approximate value of offline approved transactions in any alternate currency that was converted to the the designated currency since the counter was reset. This counter may be reset or updated during Completion Processing.
Cumulative Total Transaction Amount Upper Limit (CTTAUL), '9F5C' or 'DF31' in 'BF58'	A Visa proprietary data element indicating the maximum total accumulated amount of offline approved transactions in either the designated currency (Application Currency Code) or in any alternate currency that was converted to an approximate value in the designated currency since the counter was reset. If exceeded, an offline decline is requested.
Cumulative Total Transaction Amount x (CTTA x), 'DF1x' in 'BF58' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTTA x: CTTA 1, CTTA 2, CTTA 3, CTTA 4. The issuer Personalizes the Profile Control for the transaction to configure the counter-related behavior for each CTTA x in the Profile.
Cumulative Total Transaction Amount Upper Limit x (CTTAUL x), 'DF3X' in 'BF58' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, the application is capable of supporting multiple CTTAUL x: CTTAUL 1, CTTAUL 2, CTTAUL 3, CTTAUL 4. Each CTTAUL x is used as the upper limit for the corresponding CTTA x.
Currency Conversion Factor x *for minimum implementations of currency conversion, x = 1 to 5*	A decimal value used in the currency conversion algorithm to convert the value of an amount in the Conversion Currency to the designated currency in which the account is managed (identified by the Application Currency Code). This converted value is only used for comparisons and incrementing counters. The Amount, Authorized remains in the Transaction Currency. The Currency Conversion Factor x may be updated using an Issuer Script Command to the Currency Conversion Parameters data element. Because this rate is intended to be an approximation, update should not be necessary unless major currency fluctuations occur.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (6 of 8)

Data Element	Description
Currency Conversion Parameters, '9F73'	A constructed data element listing the currencies that may be used for currency conversion and the associated conversion rate for each currency. Currency. Consists of one to five convertible currency entries. Each convertible currency entry consists of a Conversion Currency Code x and the associated Currency Conversion Factor x (the values of "x" match). The Currency Conversion Factor x is used to approximate the value of a transaction in a designated alternate currency (Conversion Currency x) converted to the designated currency in which the account is managed (Application Currency). ***Note:*** *The "x" is not related to Profiles Functionality, it is used to associate the Currency Conversion Factor x with the Conversion Currency Code x for which the factor is used.*
Dynamic Data Authentication Failure Indicator	An internal application indicator that indicates that DDA or CDA failed during the current transaction or on a previous transaction that was declined offline.
Issuer Application Data (IAD), '9F10' • Card Verification Results (CVR)	Contains proprietary application data for transmission to the issuer. This includes the CVR. • A Visa proprietary data element containing indicators that are set based upon the results of offline processing for current and previous transactions. Sent to the issuer in the GENERATE AC response.
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, '9F56'	An indicator designating Issuer Authentication as mandatory or optional when Issuer Authentication is supported. When Issuer Authentication is set as mandatory, the card shall 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 Authentication Was Performed Using EXTERNAL AUTHENTICATE Command Indicator	Indicates whether Issuer Authentication was already performed during the current transaction using the EXTERNAL AUTHENTICATE command. This indicator is used during Completion processing to ensure the application does not perform Issuer Authentication again for the same transaction as part of processing the second GENERATE AC command.
Issuer Country Code, '9F57'	Indicates the country of the issuer.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (7 of 8)

Data Element	Description
Issuer Script Command Counter	An internal application counter used by the card to count Issuer Script Commands as follows: • If the counter is not cyclic: – it counts the number of Issuer Script commands containing secure messaging that were received by the card since the counter was last reset – the counter may be reset during completion – when the counter has reached the maximum value, this 4-bit counter remains set to 'F'. • If the counter is cyclic: – it counts Issuer Script commands that were successful – it counts continuously without resetting – when the counter has reached the maximum value, this 4-bit counter rolls over from 'F' to '0'.
Issuer Script Failure Indicator	An internal application indicator which indicates that Issuer Script has failed during the current or a previous transaction, and is reset during Completion of an online transaction where issuer authentication requirements are met.
Last Online ATC Register, '9F13'	ATC value of the last transaction that was authorized online and satisfied Issuer Authentication requirements.
Last Successful Issuer Update ATC Register	ATC value of the last transaction that was authorized online and where either Issuer Authentication was successful or an issuer script command was successfully processed.
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.
PIN Try Counter, '9F17'	Indicates the number of PIN tries remaining.
PIN Try Limit	Indicates the issuer-specified maximum number of consecutive incorrect PIN tries allowed.
Profile Control x, 'DF1X' in 'BF59' *for minimum implementations of Profiles Functionality, x = 1 to 4*	If Profiles Functionality is supported, a data element that indicates the profile-specific data and behavior options chosen by the issuer to be used for transactions processed using the profile identified by Profile ID = x. The Profile Control x associated with the Profile ID chosen during Initiate Application Processing is referred to as “the Profile Control chosen for the transaction”.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-1: Completion—Card Data (8 of 8)

Data Element	Description
Profile ID	If Profiles Functionality is supported, an identifier selected during Initiate Application Processing to identify the profile to be used for processing transactions that take place in an issuer-defined transaction environment.
Static Data Authentication Failure Indicator	An internal application indicator that indicates that SDA failed during the current transaction or on a previous transaction that was declined offline.
VLP Available Funds, '9F79' or 'DF51' in 'BF55'	Amount remaining for low-value offline contactless transactions.
VLP Funds Limit, '9F77' or 'DF71' in 'BF55'	The issuer limit for VLP Available Funds.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.2 Terminal Data

The card uses the terminal data elements described in Table 13.2 for Completion. They are passed to the card in the second GENERATE AC command if their tag and length were included in the CDOL2 read from the card during Read Application Data. The CDOL2 requirements are described in Table 13-1.

For a detailed description of these data elements and their usage, see Appendix A, VIS Data Element Tables.

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

Data Element	Description
Amount, Authorized, '9F02'	The amount of the current transaction
Authorization Response Code	Provided to the card to indicate the disposition of the transaction • Y3 = Unable to go online (offline approved) • Z3 = Unable to go online (offline declined)
Card Status Update (CSU)	The Card Status Updates contains an indication of whether the issuer approves or declines the transaction, and the following information that may be used to initiate actions specified by the issuer: • Proprietary Authentication Data Included • PIN Try Counter • Issuer Approves Online Transaction • Card Block • Application Block • Update PIN Try Counter • Set Go Online on Next Transaction • CSU Generated by Proxy for the Issuer • Update Counters

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 13-2: Completion—Terminal Data (2 of 2)

Data Element	Description
Issuer Authentication Data, '91'	Data that the terminal includes in the GENERATE AC command sent to the card if Issuer Authentication is supported (the Issuer Authentication Indicator is present), but the AIP indicates Issuer Authentication is not supported using the EXTERNAL AUTHENTICATE command. For CVN 10, the application uses the following data elements contained within the Issuer Authentication Data: • Authorization Response Cryptogram (ARPC) — An 8-byte cryptogram generated by the issuer host (or its agent) and passed to the terminal in the online response. • ARPC Response Code —The 2-byte response code indicating the issuer's decision regarding the outcome of the online authorization. It is used in the calculation of the ARPC and passed to the terminal in the online response from the issuer. Other Visa documentation also refers to this data element as the Authorization Response Code. *Optional issuer data is not supported for C*VN *10.* For CVN 18, the application uses the following data elements contained within the Issuer Authentication Data: • Authorization Response Cryptogram (ARPC)— A 4-byte cryptogram generated by the issuer host (or its agent) and passed to the terminal in the online response. • Card Status Update (CSU) — A 4-byte data element that indicates whether the issuer approves or declines the transaction, and indicators used to initiate actions specified by the issuer to update the card or application. • Proprietary Authentication Data — An optional 1 to 8-byte data element containing additional data from the issuer sent in the online response and validated during Issuer Authentication. The use of this additional data is beyond the scope of this specification.
Terminal Verification Results (TVR), '95'	Used to record offline processing results, such as SDA failure or floor limit exceeded
Terminal Country Code, '9F1A'	Indicates the country where the terminal is located
Transaction Currency Code, '5F2A'	Indicates the currency code of the transaction

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Note: *If the length of a data element requested by the card using the CDOL2 is different from the length of that data element in the terminal, the terminal truncates or pads the terminal data according to rules specified in EMV before sending the data to the card. If a data element requested using CDOL2 is not present in the terminal, the terminal sends hexadecimal zeros in place of the requested data.*

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 *EMV Book 3*, Table 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 Application Data with the CVR indicating processing results.

13.4 Completion Processing Overview and Flow

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

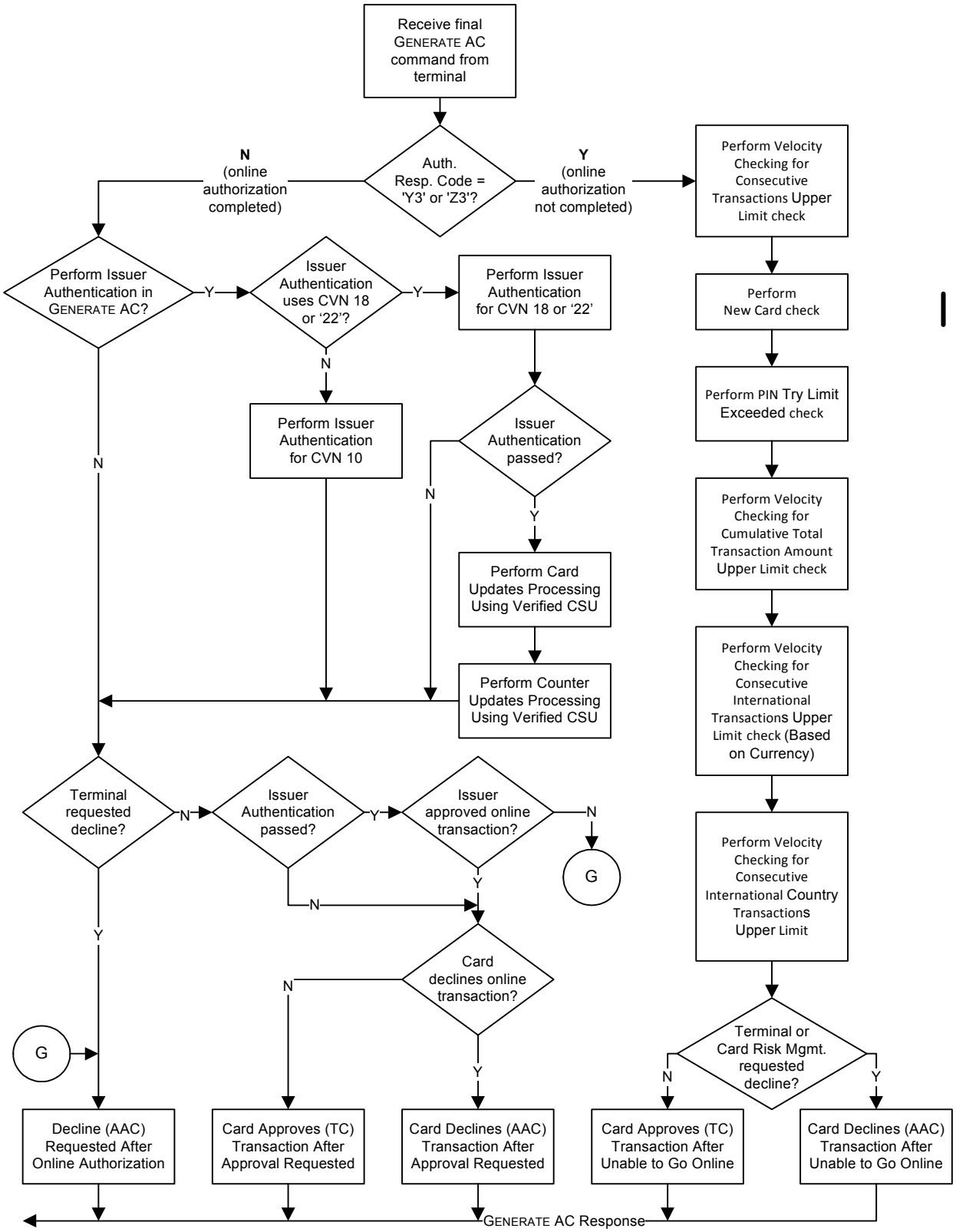
At the end of Card Action Analysis, the card may have:

- 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure 13-1: Completion Processing Flow



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.5 Receive GENERATE AC Command

Completion processing for the card occurs when the card receives the second GENERATE AC command from the terminal.

If the application is permanently blocked because the ATC has reached its maximum value, the card does not generate an Application Cryptogram or dynamic signature, discontinues processing the GENERATE AC command, and returns SW1 SW2 = '6985' (see section C.6.1).

Note: *A permanently blocked application should not receive any GENERATE AC commands.*

If the application is blocked, the card shall decline the transaction by setting the CID and CVR bits to indicate that an AAC is being returned in the second GENERATE AC response before generating the Application Cryptogram, and may skip all other second GENERATE AC command processing.

If the length of data received in the GENERATE AC command from the terminal is different from the length of data expected by the card, the card should discontinue processing the GENERATE AC command and should return an SW1 SW2 error code to the terminal. The SW1 SW2 error code should be '6700' (Wrong Length).

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 continues as described in section 13.6.
- 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 13.8.

13.6 Processing Response Data for Online Authorized Transaction

The online response from the issuer may contained Issuer Authentication Data, which may be authenticated either prior to Completion processing using the EXTERNAL AUTHENTICATE command or as part of Completion processing

If Issuer Authentication is not supported in the application, then Completion processing shall continue as described in section 13.7.

If the Issuer Authentication Data contains all zeroes, then the terminal did not receive the Issuer Authentication Data in the online response. The card shall not perform Issuer Authentication as part of second GENERATE AC command processing, and Completion Processing shall continue as described in section 13.7.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If the card performed Issuer Authentication using the EXTERNAL AUTHENTICATE command for the same transaction (that is, the Issuer Authentication Was Performed Using the EXTERNAL AUTHENTICATE Command Indicator has the value 1b), the card shall not also perform Issuer Authentication again as part of second GENERATE AC command processing of the same transaction. The card shall use the Issuer Authentication results from EXTERNAL AUTHENTICATE command processing, and Completion Processing continues as described in section 13.7.

If all of the following are true, then processing continues as described in section 13.6.1:

- the application supports Issuer Authentication (the Issuer Authentication Indicator is present)
- the Application Cryptogram is generated using CVN 10
- the Issuer Authentication Was Performed Using EXTERNAL AUTHENTICATE Command Indicator has the value 0b
- the Issuer Authentication Data does not contain all zeroes

If the application supports Issuer Authentication and the Issuer Authentication Data for CVN 18 does not contain all zeroes, then processing continues as described in section 13.6.2.

13.6.1 Issuer Authentication During Second GENERATE AC for CVN 10

For CVN 10, the card shall perform Issuer Authentication during the second GENERATE AC command using the following steps:

1. Parse out the ARPC Response Code portion of the Issuer Authentication Data for CVN 10 and store it for later use during the Completion processing in section 13.7.
2. Generate an Authorization Response Cryptogram (ARPC) from the ARPC Response Code in step 1 and the ARQC returned with the first GENERATE AC response using the algorithm described in section D.3.3, Generating the Authorization Response Cryptogram (ARPC) for CVN 10 ('0A'), and the Unique DEA Keys (UDKs) stored in the card for the application.
3. Compare the generated ARPC to the ARPC received in the GENERATE AC command. If they are the same, then Issuer Authentication is considered successful. If they differ, then Issuer Authentication has failed.

If Issuer Authentication is successful, then the card shall:

- set the Issuer Authentication Failure Indicator to 0b.
- if the card supports contactless issuer update processing, set the Last Successful Issuer Update ATC Register to the value of the ATC.
- use the ARPC Response Code that was verified by Issuer Authentication passing when processing the transaction as described in section 13.7.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If Issuer Authentication fails, then the card shall:

- set the Issuer Authentication Failure Indicator to 1b.
- set the ‘Issuer Authentication performed and failed’ bit of the CVR to 1b.
- not use the ARPC Response Code received from the terminal when processing the transaction as described in section 13.7.

The processing of these transactions continues as described in section 13.7.

13.6.2 Issuer Authentication for CVN 18 and CVN '22'

For CVN 18 and CVN '22', the Issuer Authentication Data includes the Authorization Response Cryptogram (ARPC) and the Card Status Updates (CSU), and optionally includes the Proprietary Authentication Data.

The card shall perform Issuer Authentication for CVN 18 and CVN '22' during the second GENERATE AC command using the following steps:

1. Parse out the Authorization Response Cryptogram (ARPC) portion of the Issuer Authentication Data for CVN 18 and CVN '22'.
   - Generate an ARPC from the following input data using the ARPC algorithm and session key derivation method described in section D.4:
     - ARQC returned with the first Generate AC response
     - CSU received in the Issuer Authentication Data portion of the second GENERATE AC command data
     - If the ‘Proprietary Authentication Data included’ bit of the CSU is 1b, the Proprietary Authentication Data received in the Issuer Authentication Data portion of the second GENERATE AC command data.
2. Compare the generated ARPC to the ARPC received in the Issuer Authentication Data of the second GENERATE AC command.

   If the generated ARPC and the ARPC received in the GENERATE AC command data are the same, then Issuer Authentication is considered successful; and the card shall:

   - set the Issuer Authentication Failure Indicator to 0b
   - use the ‘Issuer approves online transaction’ bit of the CSU verified by issuer authentication passing when processing the transaction as described in section 13.7.
   - if the card supports contactless issuer update processing, set the Last Successful Issuer Update ATC Register to the value of the ATC.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– continue processing the transaction as described in section 13.6.2.1, Card Updates Processing Using the Verified CSU.

If the generated ARPC and the ARPC received in the GENERATE AC command data are not the same, then Issuer Authentication has failed; and the card shall:

– set the Issuer Authentication Failure Indicator to 1b.

– set the 'Issuer Authentication performed and failed' bit of the CVR to 1b.

– not use the 'Issuer approves online transaction' bit received in the CSU when processing the transaction as described in section 13.7.

– Continue processing the transaction as described in section 13.7

13.6.2.1 Card Updates Processing Using the Verified CSU

After successful Issuer Authentication for cryptograms that use CSU processing (for example, CVN 18), the card has verified that the CSU received in Issuer Authentication Data is valid. The validated CSU contains an indicator that identifies whether the transaction is approved, and indicators for updates to the application.

The indicators in the CSU are used to update the card as follows:

- If the 'Card Block' bit in the verified CSU has the value 1b; then the card shall be blocked as described in sections 14.5.3 and C.4.

  Note: *The card block becomes effective on the next attempted transaction.*

- If the 'Application Block' bit in the verified CSU has the value 1b; then the application shall be blocked as described in sections 14.5.1 and C.2.

  The card and terminal shall continue to process the current transaction through Completion, including any issuer script command processing after the second GENERATE AC.

  Note: *The application block becomes effective on the next attempted transaction. The card is not required to return an AAC in response to the current GENERATE AC command.*

- If the 'Update PIN Try Counter' bit in the verified CSU has the value 1b, then:

  – If the value in the 'PIN Try Counter' bits of the verified CSU is greater than the PIN Try Limit, then the application shall set the PIN Try Counter to the value of the PIN Try Limit.

  – If the value in the 'PIN Try Counter' bits of the verified CSU is less than or equal to the PIN Try Limit:

    - If the implementation is capable of setting the PIN Try Counter to the value in the 'PIN Try Counter' bits of the verified CSU, then the application shall set the PIN Try Counter to the value in the 'PIN Try Counter' bits of the verified CSU.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Otherwise, the application shall set the PIN Try Counter to the value of the PIN Try Limit.

  Note: *If an implementation is capable of setting the PIN Try Counter to any value between zero and the PIN Try Limit (0 < value < PIN Try Limit), it must be capable of setting the PIN Try Counter to every possible value between zero and the PIN Try Limit. Issuers should only set the 'PIN Try Counter' bits of the CSU to a value that their cards are capable of supporting.*

- If the 'Set Go Online on Next Transaction' bit in the verified CSU has the value 1b, then the application shall set the 'Go Online on Next Transaction' indicator to 1b.

  If the 'Set Go Online on Next Transaction' bit in the verified CSU has the value 0b, then the application shall reset the 'Go Online on Next Transaction' indicator to 0b.

- 'CSU generated by proxy for the issuer' bit in the verified CSU:
  - If the issuer generates the CSU sent in the online response for cryptograms that use CSU processing (for example, CVN 18 or CVN '22'), then the issuer shall set the 'CSU generated by proxy for the issuer' bit in the CSU to the value 0b.
  - If the issuer does not generate the CSU, then the proxy for the issuer that provides the CSU that is sent in the online response for cryptograms that use CSU processing (for example, CVN 18 or CVN '22') shall set the 'CSU generated by proxy for the issuer' bit in the CSU to the value 1b

Continue processing the transaction as described in section 13.6.2.2

13.6.2.2 Counter Updates Processing Using the Verified CSU

1. The card determines whether to use the 'Update Counters' bits in the verified CSU or the 'Default Update Counters' bits in the ADA as the counter controls for this section as follows.
   - The 'Update Counters' bits in the verified CSU shall be used as the counter controls if *either* of the following is true:
     - The 'CSU Created by Proxy for the Issuer' bit in the verified CSU has the value 0b
     - The 'CSU Created by Proxy for the Issuer' bit in the verified CSU has the value 1b *and* the 'Use Default Update Counters in ADA if CSU is generated by a proxy' bit in the ADA is set to 0b.

     Otherwise the 'Default Update Counters' bits in the ADA shall be used as the counter controls.
2. The counter controls chosen in step 1 are used as follows:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– If Profiles Functionality is not supported *and* the counter controls chosen in step 1 indicate 'Do not update velocity-checking counters' (00b), then the following counters shall not be updated or reset:

  - Cumulative Total Transaction Amount (CTTA)
  - Consecutive Transaction Counter (CTC)
  - Consecutive Transaction Counter International (CTCI)
  - Consecutive Transaction Counter International Country (CTCIC)
  - Contactless Transaction Counter (CLTC)
  - VLP Available Funds

– If Profiles Functionality is not supported *and* the counter controls chosen in step 1 indicate 'Set velocity-checking counters to Upper Limits' (01b), then the following counters shall be updated to the value of the associated upper limit as follows:

  Note: *Issuers are cautioned that if the Upper Limit for a counter supported in the application is not present, this update will not change the value of the counter.*

  - Cumulative Total Transaction Amount (CTTA) to Cumulative Total Transaction Amount Upper Limit (CTTAUL) if the 'Do not reset CTTA during GENERATE AC' bit of the ADA is set to 0b
  - Consecutive Transaction Counter (CTC) to Consecutive Transaction Counter Upper Limit (CTCUL)
  - Consecutive Transaction Counter International (CTCI) to Consecutive Transaction International Upper Limit (CTIUL)
  - Consecutive Transaction Counter International Country (CTCIC) to Consecutive Transaction International Upper Limit (CTIUL)
  - Contactless Transaction Counter (CLTC) to Contactless Transaction Counter Upper Limit (CLTCUL)
  - If the card also supports qVSDC functionality and the 'Do not reset VLP Available Funds during GENERATE AC' bit of the ADA is set to 0b, reset VLP Available Funds to zero

– If Profiles Functionality is not supported *and* the counter controls chosen in step 1 indicate 'Reset velocity-checking counters to zero' (10b), then counters shall be reset as follows:

  - Cumulative Total Transaction Amount (CTTA) to zero if the 'Do not reset CTTA during GENERATE AC' bit of the ADA is set to 0b
  - Consecutive Transaction Counter (CTC) to zero

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Consecutive Transaction Counter International (CTCI) to zero
- Consecutive Transaction Counter International Country (CTCIC) to zero
- Contactless Transaction Counter (CLTC) to zero
- If the card also supports qVSDC functionality and the 'Do not reset VLP Available Funds during GENERATE AC' bit of the ADA is set to 0b, reset VLP Available Funds to the VLP Funds Limit

– If Profiles Functionality is not supported *and* the counter controls chosen in step 1 indicate 'Add transaction to velocity-checking counters' (11b), then the following counters shall be updated as follows:

- If the Transaction Currency Code is equal to the Application Currency Code, then increment the Cumulative Total Transaction Amount by the Amount, Authorized.
- If the Transaction Currency Code is not equal to the Application Currency Code but is equal to one of the Conversion Currency Codes in Currency Conversion Parameters, then increment the Cumulative Total Transaction Amount by the approximate value of the amount converted to the Application Currency (using the Amount, Authorized and the Currency Conversion Factor associated with the matching Conversion Currency Code).
- Increment the Consecutive Transaction Counter (CTC) by one.
- Increment the Consecutive Transaction Counter International (CTCI) by one if *either* of the following is true:
  – the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
  – the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b.
- If the Terminal Country Code is not equal to the Issuer Country Code, increment the Consecutive Transaction Counter International Country (CTCIC) by one.

– If Profiles Functionality is supported *and* the counter controls chosen in step 1 indicate 'Do not update velocity-checking counters' (00b), then the following counters shall not be updated or reset:

- any Cumulative Total Transaction Amount x
- any Consecutive Transaction Counter x
- any Consecutive Transaction Counter International x

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- any Consecutive Transaction Counter International Country x
- Contactless Transaction Counter (CLTC)
- VLP Available Funds

– If Profiles Functionality is supported *and* the counter controls indicate 'Set velocity-checking counters to Upper Limits' (01b), then the following counters shall be updated to the value of the associated Upper Limit as follows:

Note: *Issuers are cautioned that if the Upper Limit for a counter supported in the application is not present, this update will not change the value of the counter.*

- For every Cumulative Total Transaction Amount x, if the 'Allow reset of CTTA x' bit of the Profile Control for the transaction is set to 1b, then set Cumulative Total Transaction Amount x to the Cumulative Total Transaction Amount Upper Limit x.
- For every Consecutive Transaction Counter x, if the 'Allow reset of CTC x' bit of the Profile Control for the transaction is set to 1b, then set Consecutive Transaction Counter x to the Consecutive Transaction Counter Upper Limit x.
- For every Consecutive Transaction Counters International x, if the 'Allow reset of CTCI x' bit of the Profile Control for the transaction is set to 1b, then set Consecutive Transaction Counters International x to the Consecutive Transaction International Upper Limit x.
- For every Consecutive Transaction Counters International Country x, if the 'Allow reset of CTCIC x' bit of the Profile Control for the transaction is set to 1b, then set Consecutive Transaction Counters International Country x to the Consecutive Transaction International Upper Limit x.
- If the 'Allow reset of CLTC' bit of the Profile Control for the transaction is set to 1b, then set Contactless Transaction Counter (CLTC) to the Contactless Transaction Counter Upper Limit (CLTCUL).
- If the card also supports qVSDC functionality and the 'Do not reset VLP Available Funds during GENERATE AC' bit of the ADA is set to 0b and the 'Allow reset of VLP Available Funds' bit of the Profile Control for the transaction is set to 1b, then set VLP Available Funds to zero

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– If Profiles Functionality is supported *and* the counter controls chosen in step 1 indicate ‘Reset velocity-checking counters to zero’ (10b), then counters shall be reset as follows:

  - For every Cumulative Total Transaction Amounts x, if the ‘Allow reset of CTTA x’ bit of the Profile Control for the transaction is set to 1b, then reset Cumulative Total Transaction Amount x to zero.
  - For every Consecutive Transaction Counters x, if the ‘Allow reset of CTC x’ bit of the Profile Control for the transaction is set to 1b, then reset Consecutive Transaction Counter x to zero.
  - For every Consecutive Transaction Counters International x, if the ‘Allow reset of CTCI x’ bit of the Profile Control for the transaction is set to 1b, then reset Consecutive Transaction Counters International x to zero.
  - For every Consecutive Transaction Counters International Country x, if the ‘Allow reset of CTCIC x’ bit of the Profile Control for the transaction is set to 1b, then reset Consecutive Transaction Counters International Country x to zero.
  - If the ‘Allow reset of CLTC’ bit of the Profile Control for the transaction is set to 1b, then reset Contactless Transaction Counter (CLTC) to zero
  - If the card also supports qVSDC functionality and the ‘Do not reset VLP Available Funds during GENERATE AC’ bit of the ADA is set to 0b and the ‘Allow reset of VLP Available Funds’ bit of the Profile Control for the transaction is set to 1b, then reset VLP Available Funds to the VLP Funds Limit

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– If Profiles Functionality is supported *and* the counter controls chosen in step 1 indicate 'Add transaction to velocity-checking counters' (11b), then the counters shall be updated as follows:

  - For each Cumulative Total Transaction Amount x, if the 'Allow counting in CTTA x' bit of the Profile Control for the transaction is set to 1b:
    – if the Transaction Currency Code is equal to the Application Currency Code, then increment the Cumulative Total Transaction Amount x by the Amount, Authorized.
    – If the Transaction Currency Code is not equal to the Application Currency Code but is equal to one of the Conversion Currency Codes in Currency Conversion Parameters, then increment the Cumulative Total Transaction Amount x by the approximate value of the amount converted to the Application Currency (using the Amount, Authorized and the Currency Conversion Factor associated with the matching Conversion Currency Code).
  - For each Consecutive Transaction Counter x; if the 'Allow counting in CTC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter x by one
  - For each Consecutive Transaction Counter International x, increment the Consecutive Transaction Counter International x by one if *both* of the following are true:
    – the 'Allow counting in CTCI x' bit of the Profile Control for the transaction is set to 1b
    – *either* of the following is true:
      - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
      - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
  - If the Terminal Country Code is not equal to the Issuer Country Code; then for each Consecutive Transaction Counter International Country x, if the 'Allow counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter International Country x by one

3. Continue processing the transaction as described in section 13.7.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.7 Complete Response for Online Authorized Transaction

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

- If Issuer Authentication was performed for CVN 10 and passed (either using the EXTERNAL AUTHENTICATE command or as part of second GENERATE AC processing as described in section 13.6.1), the card shall use the verified ARPC Response Code as follows:
  - An ARPC Response Code of 00, 10, or 11 indicates an issuer approval.
  - An ARPC Response Code of 01 or 02 indicates an issuer referral.
  - An ARPC Response Code other than one listed above indicates an issuer decline. These transactions should be processed as though the terminal had requested a decline.
- If Issuer Authentication was performed using the CSU (for example, for CVN 18) as described in section 13.6.2 and passed, the card shall use the 'Issuer approves online transaction' bit of the verified CSU as follows:
  - If the 'Issuer approves online transaction' bit of the verified CSU is set to 1b, the issuer approved the transaction
  - If the 'Issuer approves online transaction' bit of the verified CSU is set to 0b, the issuer declined the transaction
- If the application supports Issuer Scripts and IAD Format 2, then set the 'Secure Messaging uses EMV Session key-based derivation' bit of the CVR to the value of the 'Secure Messaging uses EMV Session key-based derivation' bit in the ADA.
- Perform processing based on the value of the P1 parameter of the second GENERATE AC command:
  - Perform approval processing as described in section 13.7.2 if P1 indicates a TC (approval) was requested and, if Issuer Authentication was performed and passed, either of the following is true:
    - For CVN 10,the ARPC Response Code from the Issuer Authentication Data indicates an issuer approval or referral.
    - For cryptograms that use CSU processing (for example, CVN 18 or CVN '22'), the 'Issuer approves online transaction' bit of the CSU is set to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– Perform decline processing as described in section 13.7.1 if P1 indicates an AAC (decline) was requested; or, if Issuer Authentication was performed and passed, either of the following is true:

  - For CVN 10, the ARPC Response Code from the Issuer Authentication Data indicates a decline.
  - For cryptograms that use CSU processing (for example, CVN 18 or CVN '22'), the 'Issuer approves online transaction' bit of the CSU is set to 0b.

13.7.1 Decline Requested After Online Authorization

The card shall return an AAC if any of the following is true:

- The card receives a request for a decline (AAC) in the P1 parameter of the second GENERATE AC command
- For cards that use CVN 10, if Issuer Authentication was performed and passed, the ARPC Response Code value from within the verified Issuer Authentication Data shows an issuer decline.
- For cards using a cryptogram that uses CSU processing (for example, CVN 18 or CVN '22'), if Issuer Authentication was performed and passed, the 'Issuer approves online transaction' bit of the CSU verified using Issuer Authentication is set to 0b.

1. Prior to building the Issuer Application Data to send in the second GENERATE AC response:
   – Set bits in the CVR to indicate that an AAC is returned in the second GENERATE AC response
   – Set the 'Number of Issuer Script Commands' bits of the CVR to the value of the Issuer Script Command Counter, using the identical bit settings
   – If the Issuer Script Failure Indicator is set to 1b, then set the 'Issuer Script processing failed' bit of the CVR to 1b

     Note: *The 'Issuer Script processing failed' bit may be set in the CVR because a script failed before the second GENERATE AC command of the current transaction, or because a script failed during a previous transaction and the indicator has not yet been reset. In order to indicate to the issuer that a script failed before the second GENERATE AC command of the current transaction, the 'Issuer Script processing failed' bit in the CVR shall be set before the application determines whether to reset the Issuer Script Failure Indicator.*

   – If Issuer Authentication was not performed but Issuer Authentication is supported (the Issuer Authentication Indicator is present), set the 'Issuer Authentication not performed after online authorization' bit of the CVR to 1b
2. Prior to responding to the terminal with an AAC, the card shall:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– 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 1b

  - Not update or reset the Last Online ATC Register
  - Not update or reset the Issuer Script Command Counter if *any* of the following is true:
    – the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 1b
    – Issuer Authentication failed
    – Issuer Authentication was not performed and Issuer Authentication is mandatory.

– 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 if the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 0b.
    – Issuer Script Failure Indicator
    – Go Online on Next Transaction Indicator if either of the following is true:
      - Issuer Authentication was not performed
      - Issuer Authentication was performed and passed for cryptograms that do not use CSU processing (for example, for CVN 10).

– If Issuer Authentication was performed and passed for cryptograms that use CSU processing (for example, CVN 18 or CVN '22'), then the processing in section 13.6.2.1 and 13.6.2.2 controls updates of counters and reset of the Go Online on Next Transaction Indicator.

  Otherwise if Profiles Functionality is not supported:

  - If the 'Do not count declined transactions' bit of the ADA is set to 0b, then increment the Consecutive Transaction Counter (CTC) by one.
  - Not update or reset the following:
    – Cumulative Total Transaction Amount (CTTA)
    – Consecutive Transaction Counter International (CTCI)
    – Consecutive Transaction Counter International Country (CTCIC)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Contactless Transaction Counter (CLTC)
- VLP Available Funds

Otherwise if Profiles Functionality is supported:

- Increment each Consecutive Transaction Counter x by one if both of the following are true:
  - the ‘Do not count declined transactions’ bit of the ADA is set to 0b
  - the ‘Allow counting in CTC x’ bit of the Profile Control for the transaction is set to 1b
- Not update or reset the following:
  - Cumulative Total Transaction Amount (CTTA)
  - Consecutive Transaction Counter International (CTCI)
  - Consecutive Transaction Counter International Country (CTCIC)
  - Contactless Transaction Counter (CLTC)
  - VLP Available Funds

3. If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then prior to generating the Application Cryptogram, the Issuer Discretionary Data portion of the Issuer Application Data is built as described in Appendix J.
4. Generate the Application Cryptogram as described in Appendix D, Authentication Data, Keys and Algorithms
5. Set the type of cryptogram in the Cryptogram Information Data (CID) in the GENERATE AC response to AAC
6. If all of the following are true, then log the transaction:
   - Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
   - The ‘Include declined transactions in the transaction log’ bit of the ADA is set to 1b.
   - If Profiles Functionality is supported, the ‘Log transactions performed using this profile’ bit of the Profile Control chosen for the transaction is set to 1b.
   - If transaction logging is limited by Transaction Type; the Transaction Type is set to '00' (Purchase), '01' (Cash), or '11' (Quasi cash).
7. Return the second GENERATE AC response to the terminal (including the CID, ATC, Application Cryptogram, and Issuer Application Data).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.7.2 Approval Requested After Online Authorization

When *all* of the following are true:

- the card receives a request for an approval (TC) in the P1 parameter of the second GENERATE AC command
- *any* of the following is true:
  - if Issuer Authentication was performed and passed for CVN 10, the verified ARPC Response Code in the Issuer Authentication Data indicates an issuer approval or referral,
  - if Issuer Authentication was performed and passed for a cryptogram that uses CSU processing (for example, CVN 18 or CVN '22'), the 'Issuer approves online transaction' bit of the verified CSU is set to 1b.
  - Issuer Authentication was not performed

then the card shall:

- If Issuer Authentication was not performed but Issuer Authentication is supported (the Issuer Authentication Indicator is present), set the 'Issuer Authentication not performed after online authorization' bit of the CVR to 1b.

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 is true, then the card approves the transaction:
  - Issuer Authentication was successful.
  - Issuer Authentication is not supported (the Issuer Authentication Indicator is not present).
  - Issuer Authentication is optional (as shown in the Issuer Authentication Indicator) and was not performed.
  - Issuer Authentication failed, and the 'If Issuer Authentication performed and failed, decline transaction' bit of the ADA is set to 0b.
  - Issuer Authentication is mandatory (as shown in the Issuer Authentication Indicator) and was not performed, and the 'If Issuer Authentication is mandatory and no ARPC received, decline transaction' bit of the ADA is set to 0b.

  Processing for card approved transaction continues with section 13.7.2.1.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- **Card Declines**—If *any* of the following conditions is true, the card declines the transaction:
  - Issuer Authentication failed and the 'If Issuer Authentication performed and failed, decline transaction' bit of the ADA is set to 1b.
  - Issuer Authentication is mandatory (as shown in the Issuer Authentication Indicator) and was not performed, and the 'If Issuer Authentication is mandatory and no ARPC received, decline transaction' bit of the ADA is set to 1b.

  Processing for card declined transactions continues with section 13.7.2.2.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.7.2.1 Card Approves Transaction After Approval Requested

When the card approves the transaction, it shall:

1. Prior to building the Issuer Application Data to send in the second GENERATE AC response:
   - Set bits in the CVR to indicate that a TC is being returned in the second GENERATE AC response.
   - Set the 'Number of Issuer Script Commands' bits of the CVR to the value of the Issuer Script Command Counter, using the identical bit settings
   - If the Issuer Script Failure Indicator is set to 1b, then set the 'Issuer Script processing failed' bit of the CVR to 1b

     Note: *The 'Issuer Script processing failed' bit may be set in the CVR because a script failed before the second GENERATE AC command of the current transaction, or because a script failed during a previous transaction and the indicator has not yet been reset. In order to indicate to the issuer that a script failed before the second GENERATE AC command of the current transaction, the 'Issuer Script processing failed' bit in the CVR shall be set before the application determines whether to reset the Issuer Script Failure Indicator.*
   - Set the type of cryptogram in the Cryptogram Information Data (CID) in the GENERATE AC response to TC.
2. Reset counters and indicators based upon Issuer Authentication results and requirements as steps 2a and 2b:
   a. If Issuer Authentication either (1) failed or (2) was mandatory (as shown in Issuer Authentication Indicator) and not performed, then the card shall:
      - Not update or reset the following:
        - 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
        - Go Online on Next Transaction Indicator
        - Contactless Transaction Counter (CLTC)
        - VLP Available Funds
      - If Profiles Functionality is not supported, not update or reset the following:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - Cumulative Total Transaction Amount (CTTA)
  - Consecutive Transaction Counter International (CTCI)
  - Consecutive Transaction Counter International Country (CTCIC)
- If Profiles Functionality is not supported, then increment the Consecutive Transaction Counter (CTC) by one.
- If Profiles Functionality is supported, not update or reset the following:
  - any Cumulative Total Transaction Amount x
  - any Consecutive Transaction Counter International x
  - any Consecutive Transaction Counter International Country x
- If Profiles Functionality is supported; then for each Consecutive Transaction Counter x, if the ‘Allow counting in CTC x’ bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter x by one.
- If Issuer Authentication is mandatory and was not performed:
  - Set the Issuer Authentication Failure Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

- Set the 'Issuer Authentication not performed after online authorization' bit of the CVR to 1b if *either* of the following is true:
  - Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command (the Issuer Authentication Indicator is present and the 'Issuer Authentication supported using the EXTERNAL AUTHENTICATE command' bit in the AIP is 1b) and the card did not receive an EXTERNAL AUTHENTICATE command.
  - Issuer Authentication is supported as part of processing the second GENERATE AC command (the Issuer Authentication Indicator is present and the 'Issuer Authentication supported using the EXTERNAL AUTHENTICATE command' bit in the AIP is 0b) and Issuer Authentication was not performed.
- 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 if the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 0b.
  - Issuer Script Failure Indicator
- If Issuer Authentication was performed and passed for cryptograms that use CSU processing (for example, CVN 18 or CVN '22'), then the processing in section 13.6.2.1 and section 13.6.2.2 control updates of counters and reset of the Go Online on Next Transaction indicator.

  Otherwise if Profiles Functionality is not supported, then reset counters and indicators as follows:
  - Go Online on Next Transaction Indicator to zero
  - Consecutive Transaction Counter (CTC) to zero
  - Consecutive Transaction Counter International (CTCI) to zero
  - Consecutive Transaction Counter International Country (CTCIC) to zero
  - Cumulative Total Transaction Amount (CTTA) to zero if the 'Do not reset CTTA during GENERATE AC' bit of the ADA is set to 0b
  - Contactless Transaction Counter (CLTC) to zero

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– if the card supports qVSDC functionality *and* the 'Do not reset VLP Available Funds during GENERATE AC' bit of the ADA is set to 0b, then set VLP Available Funds to the VLP Funds Limit

Otherwise if Profiles Functionality is supported, then reset counters and indicators as follows:

– Go Online on Next Transaction Indicator to zero

– For each Consecutive Transaction Counter x; if the ‘Allow reset of CTC x’ bit of the Profile Control for the transaction is set to 1b, then reset the Consecutive Transaction Counter x to zero.

– For each Consecutive Transaction Counter International x; if the ‘Allow reset of CTCI x’ bit of the Profile Control for the transaction is set to 1b, then reset the Consecutive Transaction Counter International x to zero.

– For each Consecutive Transaction Counter International Country x; if the ‘Allow reset of CTCIC x’ bit of the Profile Control for the transaction is set to 1b, then reset the Consecutive Transaction Counter International Country x to zero

– For each Cumulative Total Transaction Amount x, if the 'Do not reset CTTA during GENERATE AC' bit of the ADA is set to 0b *and* the 'Allow reset of CTTA x' bit of the Profile Control for the transaction is set to 1b, then reset the Cumulative Total Transaction Amount x to zero

– If the ‘Allow reset of CLTC’ bit of the Profile Control for the transaction is set to 1b, then reset the Contactless Transaction Counter (CLTC) to zero

– If *all* of the following are true, then set VLP Available Funds to the VLP Funds Limit:

  • the card supports qVSDC functionality

  • the 'Do not reset VLP Available Funds during GENERATE AC' bit of the ADA is set to 0b

  • the 'Allow reset of VLP Available Funds' bit of the Profile Control for the transaction is set to 1b

- If the card supports qVSDC and the 'Restrict reset of Contactless functionality disabled bit' bit of the Application Capabilities is set to 0b, then reset the 'Contactless functionality disabled' bit of the Application Capabilities to 0b.
- Update the Last Online ATC Register to the current value of the ATC.
- If the ‘Issuer Script Command Counter is cyclic’ bit of the ADA is set to 1b, not reset the Issuer Script Command Counter.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

3. If the card supports qVSDC functionality, and all the following conditions are true, then reset the VLP Available Funds to the VLP Funds Limit used for qVSDC functionality:
   - the offline PIN was successfully verified (that is, the ‘Offline PIN verification performed’ bit in the CVR is set to 1b and the ‘Offline PIN verification failed’ bit in the CVR is set to 0b)
   - the ‘Low-value AND CTTA Check Supported’ bit in the Card Additional Processes is set to 1b
   - the ‘Reset VLP Available Funds to VLP Funds Limit whenever Offline PIN is successfully verified’ bit in the ADA is set to 1b
   - the card is not a new card (that is, the Last Online ATC is not zero)
   - if Profiles Functionality is supported, the ‘Allow reset of VLP Available Funds’ bit of the Profile Control for the transaction is set to 1b
4. If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then prior to generating the Application Cryptogram, the Issuer Discretionary Data portion of the Issuer Application Data is built as described in Appendix J.
5. Generate the Application Cryptogram as described in Appendix D, Authentication Data, Keys and Algorithms.
6. If CDA was requested in the GENERATE AC command, generate a Signed Dynamic Application Data as described in section 13.9.
7. If all of the following are true, then log the transaction:
   - Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
   - The ‘Do not include online approved transactions in the transaction log’ bit of the ADA is set to 0b.
   - If Profiles Functionality is supported, the ‘Log transactions performed using this profile’ bit of the Profile Control chosen for the transaction is set to 1b.
   - If transaction logging is limited by Transaction Type; the Transaction Type is set to '00' (Purchase), '01' (Cash), or '11' (Quasi cash).
8. Return the second GENERATE AC response to the terminal (including the CID, ATC, Application Cryptogram, and Issuer Application Data).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.7.2.2 Card Declines Transaction After Approval Requested

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

1. Prior to building the Issuer Application Data to send in the second GENERATE AC response:
   - Set bits in the CVR to indicate that an AAC is being returned in the second GENERATE AC response.
   - Set the 'Number of Issuer Script Commands' bits of the CVR to the value of the Issuer Script Command Counter, using the identical bit settings
   - If the Issuer Script Failure Indicator is set to 1b, then set the 'Issuer Script processing failed' bit of the CVR to 1b

     Note: *The 'Issuer Script processing failed' bit may be set in the CVR because a script failed before the second GENERATE AC command of the current transaction, or because a script failed during a previous transaction and the indicator has not yet been reset.*
   - Set the type of cryptogram in the Cryptogram Information Data in the GENERATE AC response to AAC.
2. If Issuer Authentication is supported and mandatory, then set the Issuer Authentication Failure Indicator to '1'.

   If the 'If transaction declined because Issuer Authentication failed or not performed, create advice' bit of the ADA is set to 1b, then set the 'Advice required' bit of the Cryptogram Information Data to 1b.

   If Profiles Functionality is not supported *and* the 'Do not count declined transactions' bit of the ADA is set to 0b, then increment the Consecutive Transaction Counter (CTC) by one.

   If Profiles Functionality is supported *and* the 'Do not count declined transactions' bit of the ADA is set to 0b; then for each Consecutive Transaction Counter x, if the 'Allow counting in CTC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter x by one.

   Not update or reset the following:
   - Cumulative Total Transaction Amount (CTTA)
   - Consecutive Transaction Counter International (CTCI)
   - Consecutive Transaction Counter International Country (CTCIC)
   - Contactless Transaction Counter (CLTC)
   - Any Cumulative Total Transaction Amount x (CTTA x)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Any Consecutive Transaction Counter International x (CTCI x)
- Any Consecutive Transaction Counter International Country x (CTCIC x)
- 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

3. If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then prior to generating the Application Cryptogram, the Issuer Discretionary Data portion of the Issuer Application Data is built as described in Appendix J.
4. Generate the Application Cryptogram as described in Appendix D, Authentication Data, Keys and Algorithms.
5. If all of the following are true, then log the transaction:
   - Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
   - The ‘Include declined transactions in the transaction log’ bit of the ADA is set to 1b.
   - If Profiles Functionality is supported, the ‘Log transactions performed using this profile’ bit of the Profile Control chosen for the transaction is set to 1b.
   - If transaction logging is limited by Transaction Type; the Transaction Type is set to '00' (Purchase), '01' (Cash), or '11' (Quasi cash).
6. Return the second GENERATE AC response to the terminal (including the CID, ATC, Application Cryptogram, and Issuer Application Data).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.8 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 13.8.1).
- Respond back to the terminal (section 13.8.2).

13.8.1 Card Risk Management

Card risk management includes optional checks to determine whether the number of offline transactions has exceeded the Upper Consecutive Offline Limit, whether the offline amount limit has been exceeded, whether the card is a new card, whether the PIN Try Limit was exceeded in a previous transaction, and whether offline PIN verification was not performed or not successful for a PIN-Expecting card.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.8.1.1 Velocity Checking for Consecutive Transactions Upper Limit

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

If Profiles Functionality is not supported and the Consecutive Transaction Counter (CTC) and Consecutive Transaction Counter Upper Limit (CTCUL) are present, then the card shall perform the following check:

- the card checks whether the sum of the CTC plus one is greater than the CTCUL if *either* of the following is true:
  - the 'Do not count declined transactions' bit of the ADA is set to 0b
  - the terminal requested an approval (TC)

  Otherwise the card checks whether the CTC is greater than the CTCUL

If Profiles Functionality is supported and the Consecutive Transaction Counter x and Consecutive Transaction Counter Upper Limit x are present, then the card shall perform the following check for each Consecutive Transaction Counter x:

- the card checks whether the sum of the Consecutive Transaction Counter x plus one is greater than the Consecutive Transaction Counter Upper Limit x if *both* of the following are true:
  - the 'Allow Counting in CTC x' bit of the Profile Control for the transaction is set to 1b
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC)

  Otherwise the card checks whether the Consecutive Transaction Counter x is greater than the Consecutive Transaction Counter Upper Limit x if *either* of the following is true:
  - the 'Allow Counting in CTC x' bit of the Profile Control for the transaction is set to 1b
  - the 'Check limits for CTC x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card shall:

- Set the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Set the Offline Decline Requested by Card Indicator to 1b to indicate that an AAC should be returned after completion of card risk management.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.8.1.2 New Card

This check is optional for the card and determines whether 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 this check is to be performed, then the Application Default Action (ADA) shall be present in the card.

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

- Set the ‘New card’ bit of the CVR to 1b.
- Set the Offline Decline Requested by Card Indicator to 1b to indicate that an AAC should be returned after completion of card risk management if either of the following is true:
  - Profiles Functionality is not supported and the ‘If new card, decline if unable to transmit transaction online’ bit of the ADA is set to 1b,
  - Profiles Functionality is supported and the ‘If new card, decline if unable to transmit transaction online’ bit of the Profile Control chosen for the transaction is set to 1b.

13.8.1.3 PIN Try Limit Exceeded

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

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

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, then the card shall:

- If the PIN Try Counter is zero and the ‘If PIN Try Limit exceeded on previous transaction, decline if unable to transmit transaction online’ bit of the ADA is set to 1b:
  - Set Offline Decline Requested by Card Indicator to 1b to indicate that an AAC should be returned after completion of card risk management.
  - Set the ‘PIN Try Limit exceeded’ bit of the CVR to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

13.8.1.4 Velocity Checking for Cumulative Total Transaction Amount Upper Limit

This optional card check declines the transaction offline if the limit set for the maximum cumulative transaction amount for consecutive offline transactions in any supported currency has been exceeded.

Note: *When Profiles Functionality is supported, the amount may be checked against the limit regardless of the transaction currency.*

When Profiles Functionality is not supported, the amount is checked against the limit only if the transaction is in the application currency or in a currency that can be approximately converted.

If Profiles Functionality is not supported and the Application Currency Code, Cumulative Total Transaction Amount (CTTA) and Cumulative Total Transaction Amount Upper Limit (CTTAUL) are present, then the card shall perform the following check:

- If the Transaction Currency Code equals the Application Currency Code, then the card checks whether the sum of the Cumulative Total Transaction Amount and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Upper Limit,

  Otherwise, if the Transaction Currency Code equals one of the Conversion Currency Codes in the Currency Conversion Parameters, then the card checks whether the sum of the Cumulative Total Transaction Amount and the approximate value of the transaction in the application currency is greater than the Cumulative Total Transaction Amount Upper Limit.

If Profiles Functionality is supported and the Application Currency Code, Cumulative Total Transaction Amount x and Cumulative Total Transaction Amount Upper Limit x are present; then the card shall perform the following check for each Cumulative Total Transaction Amount x:

- The card checks whether the sum of the Cumulative Total Transaction Amount x and the Amount, Authorized is greater than the Cumulative Total Transaction Amount Upper Limit x if *both* of the following are true:
  - the ‘Allow Counting in CTTA x’ bit of the Profile Control for the transaction is set to 1b;
  - the Transaction Currency Code equals the Application Currency Code

  Otherwise the card shall check whether the sum of the Cumulative Total Transaction Amount x and the approximate value of the transaction in the application currency is greater than the Cumulative Total Transaction Amount Upper Limit x if *both* of the following are true:
  - the ‘Allow Counting in CTTA x’ bit of the Profile Control for the transaction is set to 1b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– the Transaction Currency Code equals one of the Conversion Currency Codes in the Currency Conversion Parameters

Otherwise, the card shall check whether the Cumulative Total Transaction Amount x is greater than the Cumulative Total Transaction Amount Upper Limit x if *either* of the following is true:

– the 'Allow Counting in CTTA x' bit of the Profile Control for the transaction is set to 1b

– the 'Check limits for CTTA x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card shall:

- Set the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Set the Offline Decline Requested by Card Indicator to 1b to indicate that an AAC should be returned after completion of card risk management.

Note: *A currency conversion example is provided in section 11.4.3.*

13.8.1.5 Velocity Checking for Consecutive International Transactions Upper Limit

This check is optional for the card and determines whether the limit set for the maximum number of consecutive offline international transactions has been exceeded. This check defines an international transaction as a transaction where the Transaction Currency Code from the terminal does not match any supported currency on the card. An issuer option allows this check to extend the definition of international transaction to also include any transaction where the Terminal Country Code does not match the Issuer Country Code (even if the currency is supported).

Note: *When Profiles Functionality is supported, the counter may be checked against the limit regardless of the transaction currency.*

When Profiles Functionality is not supported, the counter is checked against the limit if the transaction is in an international currency that cannot be converted to the application currency and optionally if the transaction is in an international country.

If Profiles Functionality is not supported and the Application Currency Code, Consecutive Transaction Counter International (CTCI) and the Consecutive Transaction International Upper Limit (CTIUL) are present; and if Consecutive International Transactions card velocity checking includes international country transactions, the Issuer Country Code is present; then the card shall perform the following check:

The card shall compare the Transaction Currency Code to the Application Currency Code and if currency conversion is supported, to the Conversion Currency Codes in the Currency Conversion Parameters.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- the card shall check whether the sum of the CTCI plus one is greater than the CTIUL if *both* of the following are true:
  - *either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
    - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC)

  Otherwise, the card shall check whether the CTCI is greater than the CTIUL if either of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
    - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b

If Profiles Functionality is supported and the Application Currency Code, Consecutive Transaction Counter International x, and Consecutive Transaction International Upper Limit x are present; and if Consecutive International Transactions card velocity checking includes international country transactions, the Issuer Country Code is present; then the card shall perform the following check for each Consecutive Transaction Counter International x:

- The card checks whether the sum of the Consecutive Transaction Counter International x plus one is greater than the Consecutive Transaction International Upper Limit x if *all* of the following are true:
  - the 'Allow Counting in CTCI x' bit of the Profile Control for the transaction is set to 1b
  - *either* of the following is true:
    - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b

– *either* of the following is true:

- the 'Do not count declined transactions' bit of the ADA is set to 0b
- the terminal requested an approval (TC)

Otherwise, the card checks whether the Consecutive Transaction Counter International x is greater than the Consecutive Transaction International Upper Limit x if *either* of the following is true:

– the 'Allow Counting in CTCI x' bit of the Profile Control for the transaction is set to 1b

– the 'Check limits for CTCI x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card shall:

- Set the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Set the Offline Decline Requested by Card Indicator to 1b to indicate that an AAC should be returned after completion of card risk management.

13.8.1.6 Velocity Checking for Consecutive International Country Transactions Upper Limit

This check is optional for the card and determines whether the limit set for the maximum number of consecutive offline international transactions (determined by country in the card application) has been exceeded.

Note: *When Profiles Functionality is supported, the counter may be checked against the limit regardless of the country in which the transaction takes place.*

When Profiles Functionality is not supported, the counter is checked against the limit only for an international country transaction.

If Profiles Functionality is not supported and the Issuer Country Code, Consecutive Transaction Counter International Country (CTCIC) and the Consecutive Transaction International Upper Limit (CTIUL) are present, then the card shall perform the following check:

- The card shall check whether the sum of the CTCIC plus one is greater than the CTIUL if *both* of the following are true:

  – the Terminal Country Code is not equal to the Issuer Country Code

  – *either* of the following is true:

    - the 'Do not count declined transactions' bit of the ADA is set to 0b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- the terminal requested an approval (TC)

Otherwise, if the Terminal Country Code is not equal to the Issuer Country Code; then the card checks whether the CTCIC is greater than the CTIUL

If Profiles Functionality is supported and the Issuer Country Code, Consecutive Transaction Counter International Country x, and Consecutive Transaction International Upper Limit x are present, then the card shall perform the following check for each Consecutive Transaction Counter International Country x:

- The card shall check whether the sum of the Consecutive Transaction Counter International Country x plus one is greater than the Consecutive Transaction International Upper Limit x if *all* of the following are true:
  - the 'Allow Counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b
  - the Terminal Country Code is not equal to the Issuer Country Code
  - *either* of the following is true:
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - the terminal requested an approval (TC)

  Otherwise, the card shall check whether the Consecutive Transaction Counter International Country x is greater than the Consecutive Transaction International Upper Limit x if *either* of the following is true:
  - the 'Allow Counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b
  - the 'Check limits for CTCIC x' bit of the Profile Control for the transaction is set to 1b.

If any of the velocity checking limits have been exceeded, then the card shall:

- Set the 'Exceeded velocity checking counters' bit of the CVR to 1b.
- Set the Offline Decline Requested by Card Indicator to 1b to indicate that an AAC should be returned after completion of card risk management.

13.8.1.7 PIN Verification Not Performed or Failed for a PIN-Expecting Card

This optional check for cards supporting Offline PIN verification declines offline if the issuer wanted the card to go online for authorization when Offline (plaintext or enciphered) PIN was not performed or was not successful.

If this check is to be performed, then if *either* of the following is true:

- The 'If Offline PIN verification not performed, decline if unable to transmit transaction online' bit of the ADA is set to 1b *and* the 'Offline PIN verification performed' bit of the CVR is set to 0b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- The ‘If Offline PIN verification not successful, decline if unable to transmit transaction online’ bit of the ADA is set to 1b *and* the ‘Offline PIN verification failed’ bit of the CVR is set to 1b

then the card shall set the Offline Decline Requested by Card Indicator to 1b.

13.8.2 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 *any* of the following conditions is 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'
- The card is an online-only card.

This decline processing is described in section 13.8.2.1.

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 1b

This approval processing is described in section 13.8.2.2.

13.8.2.1 Card Declines (AAC) 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 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 ‘SDA failed’ bit of the TVR is set to 1b, set the Static Data Authentication Failure Indicator to 1b.
- If the ‘DDA failed’ bit of the TVR is set to 1b, set the Dynamic Data Authentication Failure Indicator to 1b.
- If the ‘CDA failed’ bit of the TVR is set to 1b, set the Dynamic Data Authentication Failure Indicator to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- If Profiles Functionality is not supported, increment counters (if present) as follows:
  - If the Terminal Country Code is not equal to the Issuer Country Code, and the 'Do not count declined transactions' bit of the ADA is set to 0b, increment the Consecutive Transaction Counter International Country (CTCIC) by one.
  - Increment the Consecutive Transaction Counter International (CTCI) by one if *both* of the following are true:
    - *either* of the following is true:
      - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
      - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
    - the 'Do not count declined transactions' bit of the ADA is set to 0b.
  - If the 'Do not count declined transactions' bit of the ADA is set to 0b, increment the Consecutive Transaction Counter (CTC) by one.
- If Profiles Functionality is supported, increment counters (if present) as follows:
  - If the Terminal Country Code is not equal to the Issuer Country Code, *and* the 'Do not count declined transactions' bit of the ADA is set to 0b; then for each Consecutive Transaction Counter International Country x, if the 'Allow counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter International Country x by one
  - For each Consecutive Transaction Counter International x, increment the Consecutive Transaction Counter International x by one of *all* of the following are true:
    - *either* of the following is true:
      - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
      - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
    - the 'Do not count declined transactions' bit of the ADA is set to 0b
    - if the 'Allow counting in CTCI x' bit of the Profile Control for the transaction is set to 1b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - If the ‘Do not count declined transactions’ bit of the ADA is set to 0b; then for each Consecutive Transaction Counter x, if the ‘Allow counting in CTC x’ bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter x by one

- If the ‘If transaction declined offline, create advice’ bit of the ADA is set to 1b, set the ‘Advice required’ bit of the Cryptogram Information Data to 1b.
- Do not update the Last Online ATC Register.
- If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then prior to generating the Application Cryptogram, the Issuer Discretionary Data portion of the Issuer Application Data is built as described in Appendix 13.
- Generate an Application Cryptogram as described in Appendix D, Authentication Data, Keys and Algorithms.
- Set the type of cryptogram in the Cryptogram Information Data in the GENERATE AC response to AAC.
- If all of the following are true, then log the transaction:
  - Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
  - The ‘Include declined transactions in the transaction log’ bit of the ADA is set to 1b.
  - If Profiles Functionality is supported, the ‘Log transactions performed using this profile’ bit of the Profile Control chosen for the transaction is set to 1b.
  - If transaction logging is limited by Transaction Type; the Transaction Type is set to '00' (Purchase), '01' (Cash), or '11' (Quasi cash).
- Return the second GENERATE AC response to the terminal (including the CID, ATC, Application Cryptogram, and Issuer Application Data).

13.8.2.2 Card Approves (TC) 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 Profiles Functionality is not supported, the card updates counters, if present, as follows:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- Increment the Consecutive Transaction Counter (CTC) by one.
- If the Terminal Country Code is not equal to the Issuer Country Code, increment the Consecutive Transaction Counter International Country (CTCIC) by one.
- If the Transaction Currency Code is equal to the Application Currency Code, then increment the Cumulative Total Transaction Amount by the Amount, Authorized.
- Increment the Consecutive Transaction Counter International (CTCI) by one if *either* of the following is true:
  - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
  - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
- If the Transaction Currency Code is not equal to the Application Currency Code but is equal to one of the Conversion Currency Codes in Currency Conversion Parameters, then increment the Cumulative Total Transaction Amount by the approximate value of the amount converted to the Application Currency (using the Amount, Authorized and the Currency Conversion Factor associated with the matching Conversion Currency Code).

- If Profiles Functionality is supported, the card updates counters, if present, as follows:
  - For each Cumulative Total Transaction Amount x, if the 'Allow counting in CTTA x' bit of the Profile Control for the transaction is set to 1b:
    - if the Transaction Currency Code is equal to the Application Currency Code, then increment the Cumulative Total Transaction Amount by the Amount, Authorized.
    - If the Transaction Currency Code is not equal to the Application Currency Code but is equal to one of the Conversion Currency Codes in Currency Conversion Parameters, then increment the Cumulative Total Transaction Amount by the approximate value of the amount converted to the Application Currency (using the Amount, Authorized and the Currency Conversion Factor associated with the matching Conversion Currency Code).
  - For each Consecutive Transaction Counter x; if the 'Allow counting in CTC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter x by one

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - For each Consecutive Transaction Counter International x, increment the Consecutive Transaction Counter International x by one if *both* of the following are true:
    - *either* of the following is true:
      - the Transaction Currency Code is not equal to the Application Currency Code nor to any of the Conversion Currency Codes in Currency Conversion Parameters
      - the Terminal Country Code does not match the Issuer Country Code and the 'CTCI also counts non-matching country code transactions' bit of the ADA is set to 1b
    - the 'Allow counting in CTCI x' bit of the Profile Control for the transaction is set to 1b.
  - If the Terminal Country Code is not equal to the Issuer Country Code; then for each Consecutive Transaction Counter International Country x, if the 'Allow counting in CTCIC x' bit of the Profile Control for the transaction is set to 1b, then increment the Consecutive Transaction Counter International Country x by one

- If the card supports qVSDC functionality, and all the following conditions are true, then reset the VLP Available Funds to the VLP Funds Limit used for qVSDC functionality:
  - the offline PIN was successfully verified (that is, the 'Offline PIN verification performed' bit in the CVR is set to 1b and the 'Offline PIN verification failed' bit in the CVR is set to 0b)
  - the 'Low-value AND CTTA Check Supported' bit in the Card Additional Processes is set to 1b
  - the 'Reset VLP Available Funds to VLP Funds Limit whenever Offline PIN is successfully verified' bit in the ADA is set to 1b
  - the card is not a new card (that is, the Last Online ATC is not zero)
  - if Profiles Functionality is supported, the 'Allow reset of VLP Available Funds' bit of the Profile Control for the transaction is set to 1b
- Do not update the Last Online ATC Register.
- If sending Issuer Discretionary Data in the Issuer Application Data is supported as described in Appendix J, Issuer Discretionary Data Options, then prior to generating the Application Cryptogram, the Issuer Discretionary Data portion of the Issuer Application Data is built as described in Appendix J.
- Generate an Application Cryptogram as described in Appendix D, Authentication Data, Keys and Algorithms.
- Set the type of cryptogram in the Cryptogram Information Data in the GENERATE AC response to TC.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- If CDA was requested in the GENERATE AC command, generate a Signed Dynamic Application Data as described in section 13.9.
- If all of the following are true, then log the transaction:
  - Transaction logging is supported and uses ADA byte 3 bits 8-6 to determine which transactions are logged.
  - The 'Do not include offline approved transactions in the transaction log' bit of the ADA is set to 0b.
  - If Profiles Functionality is supported, the 'Log transactions performed using this profile' bit of the Profile Control chosen for the transaction is set to 1b.
  - If transaction logging is limited by Transaction Type; the Transaction Type is set to '00' (Purchase), '01' (Cash), or '11' (Quasi cash).
- Return the second GENERATE AC response to the terminal (including the CID, ATC, Application Cryptogram, and Issuer Application Data).

13.9 CDA Requested

Upon determining that the terminal is requesting CDA and the transaction is being approved, the card shall generate a dynamic signature from the Application Cryptogram as described in *EMV Book 2*, section 6.6.1 and summarized in the next five steps:

1. Apply the SHA-1 algorithm to a concatenation of the following data to form the Transaction Data Hash Code:
   - The values in the data elements sent by the terminal in the GET PROCESSING OPTIONS command
   - The values sent by the terminal in the first GENERATE AC command
   - The values sent by the terminal in the second GENERATE AC command
   - The tags, lengths, and values of the data elements to be returned by the ICC in the response to the second GENERATE AC command in the order they are returned, with the exception of the Signed Dynamic Application Data.
2. Concatenate the data indicated in *EMV Book 2*, Table 17. This data includes the ICC Dynamic Data which (as shown in *EMV Book 2*, Table 18) contains the ICC Dynamic Number Length, ICC Dynamic Number, Cryptogram Information Data, Application Cryptogram (TC), and Transaction Data Hash Code.
3. Generate the hash value from the concatenated data.
4. Include the hash in the Signed Dynamic Application Data.
5. Sign the Signed Dynamic Application Data with the ICC Private Key.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Include the signature of the Signed Dynamic Application Data in the GENERATE AC response.

13.10 Prior Related Processing

Initiate Application Processing

If the Profiles Functionality is supported, Profile Selection determines the Profile ID that identifies which Profile Control x to use for customizing processing of the transaction for the specific transaction environment.

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, then the ARPC in that command is validated and indicators are set for Issuer Authentication performed and passed or for Issuer Authentication performed and failed.

13.11 Subsequent Related Processing

Card Action Analysis (Subsequent Transactions)

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14 Issuer-to-Card Script Processing

Issuer-to-Card Script Processing provides a mechanism for 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 *EMV Book 3*, section 10.10, and *EMV Book 4*, section 6.3.9.

Issuer Script commands provide methods 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 includes the following sections:

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14.1 Key Management for Issuer Script Processing

Issuer-to-Card Script Processing uses unique cryptographic keys to provide message authentication and 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 Issuer Script Commands.
- **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 commands that require secure messaging, such as Issuer Script Commands.

  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 Data, Keys and Algorithms.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

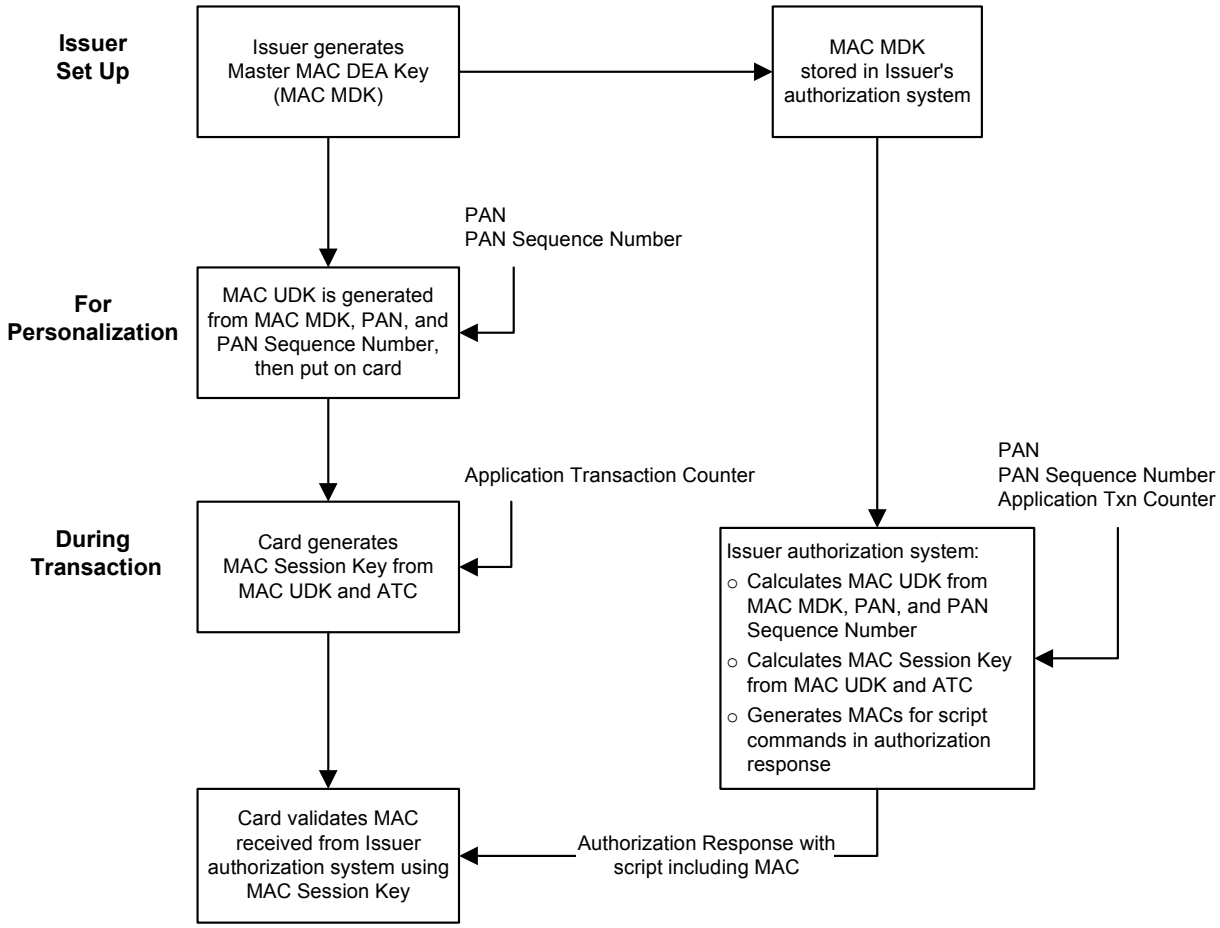
- **MAC Session Key**—A transaction-unique key which is generated by the issuer host during online transactions and is used to calculate a MAC value which is included in the Issuer Script. When the card receives the script, it generates the MAC Session Key from the MAC UDK and uses it to recalculate 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure 14-1: Generation and Use of MAC Keys



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

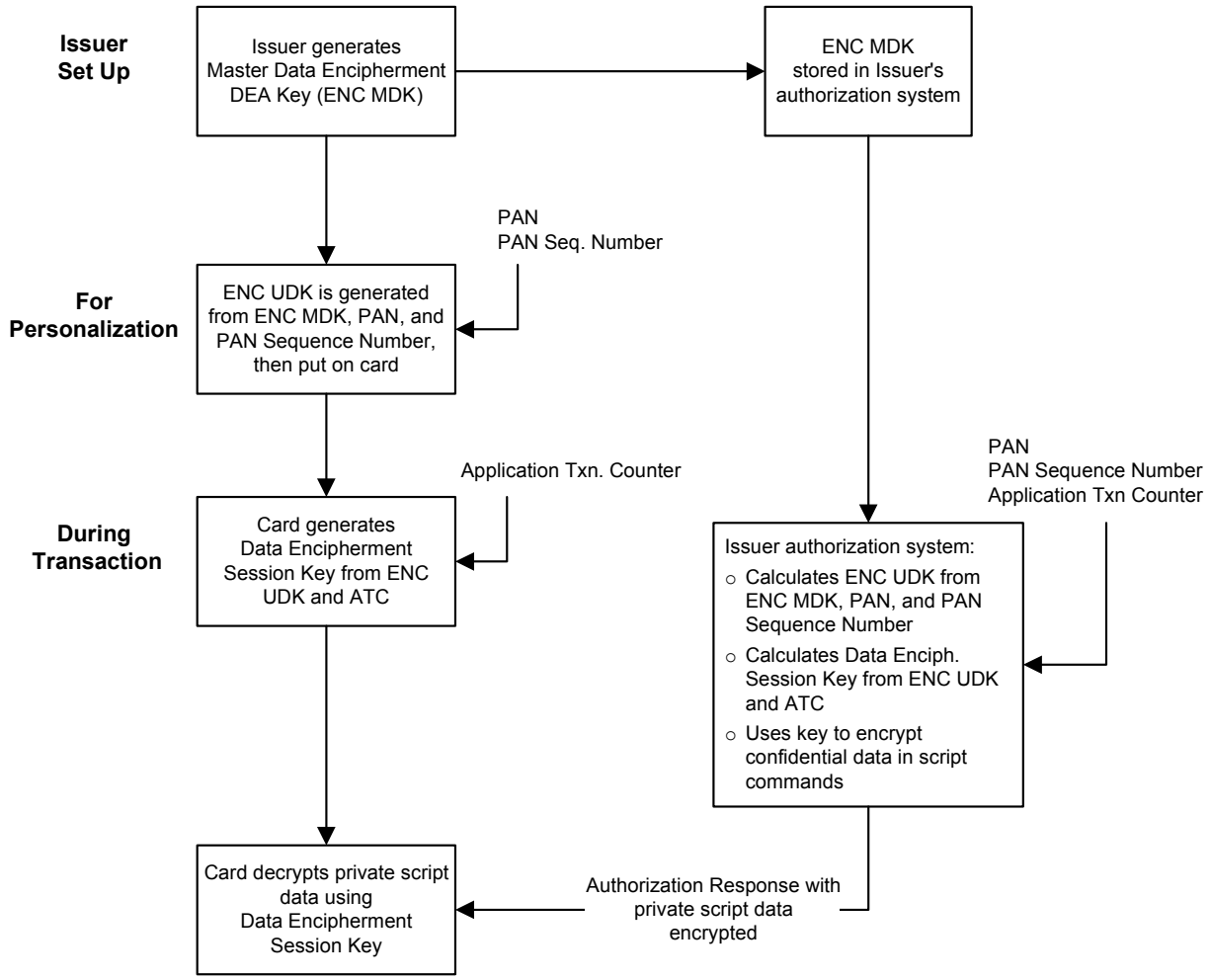
  The Data Encipherment DEA Key (ENC UDK) is a double-length DES key comprised of the Data Encipherment DEA Key A and Key B. The method for generating the ENC UDK is the same method used for the Unique DEA key and is described in Appendix D, Authentication Data, Keys and Algorithms.
- **Data Encipherment 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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

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



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, VIS Data Element Tables.

Table 14-1: Issuer-to-Card Script Processing—Card Data (1 of 2)

Data Element	Description
Application Cryptogram, '9F26'	A cryptogram returned by the ICC in the response of the GENERATE AC command (that is, a TC, ARQC, or AAC), which may be used for Issuer script MAC generation.
Application Transaction Counter (ATC), '9F36'	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 bits: • 'Number of Issuer Script Commands'—Contains value from Issuer Script Command Counter. • 'Issuer Script processing failed'—Set to 1b if the Issuer Script Failure Indicator is set to 1b. ***Note:*** *If the 'Issuer Script processing failed' bit is set in the CVR of a first GENERATE AC command, then on a previous transaction either a script failed before the second GENERATE AC command and issuer authentication requirements were not met to reset the indicator, or a script failed after the second GENERATE AC command.* ***Note:*** *If the 'Issuer Script processing failed' bit is set in the CVR of a second GENERATE AC command, either the script failed on a previous transaction and the indicator has not yet been reset, or a script failed before the second GENERATE AC command of the current transaction.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table 14-1: Issuer-to-Card Script Processing—Card Data (2 of 2)

Data Element	Description
Issuer Script Command Counter	An internal application counter used by the card to count Issuer script commands (regardless of whether they are received before or after the second GENERATE AC command) as follows: • If the Issuer Script Command Counter is not cyclic: – it counts the number of Issuer Script commands containing secure messaging that were received by the card since the counter was last reset – the counter may be reset during completion – when the counter has reached the maximum value, this 4-bit counter remains set to 'F'. • If the Issuer Script Command Counter is cyclic: – it counts Issuer Script commands that were successful – it counts continuously without resetting – when the counter has reached the maximum value, this 4-bit counter rolls over from 'F' to '0'.
Issuer Script Failure Indicator	The card shall set the Issuer Script Failure Indicator to 1b if one of the following error conditions occurs during card processing of an issuer script command received before or 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. This indicator may be reset during Completion of either the current transaction (if the issuer script command is received before the second GENERATE AC command) or a subsequent transaction.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, see Appendix A, VIS Data Element Tables.

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

Data Element	Description
Issuer Script Results, '9F5B'	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), '95'	The TVR contains two script-related indicators: • Issuer Script processing failed before final GENERATE AC command • Issuer Script processing failed after final GENERATE AC command
Transaction Status Information (TSI), '9B'	The TSI contains a flag indicating that Issuer Script processing was performed

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

The Issuer Script format is described in detail in *EMV Book 3*, section 10.10.

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

Data Element	Description
Issuer Script Template, '71' or '72'	Use of Issuer Script Template 2 is strongly recommended. Tag '72' identifies Issuer Script Template 2, which contains proprietary issuer data for transmission to the card after the second GENERATE APPLICATION CRYPTOGRAM (AC) command. Use of Issuer Script Template 1 is not recommended, but is allowed if the issuer has a strong business need to update the card before processing the second GENERATE AC command. Tag '71' identifies Issuer Script Template 1, which contains proprietary issuer data for transmission to the card before the second GENERATE AC command.
Issuer Script Identifier, '9F18'	The Issuer Script Identifier is a number used by the issuer to uniquely identify the Issuer Script.
Issuer Script Commands, '86'	Each Issuer Script Command in the script is in BER-TLV format with tag '86'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 implement these functions are described in detail in *EMV Book 3*, section 6.5, 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.

14.5.1 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 but the ATC has not reached its maximum value, 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, then 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, then 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 *VSDC Personalization Specification*.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14.5.2 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, then 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 *VSDC Personalization* Specification.

14.5.3 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. 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, then the card and terminal shall continue to process the transaction through to Completion, including processing any issuer script commands received during the same transaction. 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, then 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14.5.4 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, then all PIN data shall be enciphered using Data Encryption Algorithm (DEA) in accordance with ISO 9564. The encipherment method is described in section 14.6.3, 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.

14.5.5 PUT DATA

The PUT DATA command allows specific primitive and constructed 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.

Section A-1 indicates those data elements that may be updated using the PUT DATA command. If the Update column in Table A-1 indicates that no update is allowed, issuer script updates to the data element using PUT DATA shall not be allowed.

Appendix C describes special functionality associated with using PUT DATA for specific data elements.

14.5.6 UPDATE RECORD

The UPDATE RECORD command is used to update a record in a file with the data provided in the command data field. Visa recommends storing data which may be updated using the UPDATE RECORD command in separate records than those used for data that will not be updated.

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 if these limits are stored in files identified by SFIs 1–10 to support terminal velocity checking.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 may have tag '71' (for Issuer Script Template 1) indicating that Issuer Script processing is to be performed before the second GENERATE AC command, or tag '72' (for Issuer Script Template 2) indicating that Issuer Script processing is to be performed after the second GENERATE AC command. Use of Issuer Script Template 2 is strongly recommended over the use of Issuer Script Template 1.

At most one Issuer Script Template is transmitted in the response message. (In a subsequent version of this specification, issuers may be permitted to transmit more than one Issuer Script Template.) A script may contain multiple commands.

The Issuer Script Template is not sent to the card. The terminal sends each Issuer Script Command contained within the Issuer Script Template to the card as a separate command either before or after the second GENERATE AC command, depending on whether the Issuer Script Template in the authorization response message had tag '71' or tag '72'.

The Issuer Script Commands defined in *EMV Book 3*, section 6.5, and in Appendix C, Commands for Financial Transactions, of this document are used to perform the functions described in section 14.5.

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

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 describes the setting of Visa proprietary indicators relating to Issuer Script processing when an Issuer Script Command is transmitted to the card (before or after the second GENERATE AC command).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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. However, Issuer Authentication (as described in Chapter 12, Online Processing, or in Chapter 13, Completion Processing) shall not be required to be performed and shall not be required to pass if performed for script processing to be performed.

Secure messaging shall be performed as described in *EMV 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, this section describes the use of secure messaging in the context of the processing of those Issuer Script Commands.

The principle objectives of secure messaging are 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, and in detail in Appendix B, Secure Messaging.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

14.6.4 Other Considerations

If the issuer supports cardholder-selected PINs or supports PIN change by means of the PIN CHANGE/UNBLOCK command, then 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, then the issuer shall ensure that the record in which they are stored may be updated. If updating of the record is allowed, then 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 for Script Processing

The card shall use the Issuer Script Command Counter to count Issuer Script commands, regardless of whether they were received before or after the second GENERATE AC command, as follows:

- If the counter is not cyclic (the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 0b):
  - it counts the number of Issuer Script commands containing secure messaging that were received by the card since the counter was last reset
  - the counter may be reset during completion of either the current transaction (if the issuer script command is received before the second GENERATE AC command) or a subsequent transaction (if the issuer script command is received after the second GENERATE AC command)
  - when the counter has reached the maximum value, the 4-bit counter remains set to 'F'.
- If the counter is cyclic (the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 1b):
  - it counts only Issuer Script commands that were successful
  - it counts continuously without resetting
  - when the counter has reached the maximum value, the 4-bit counter rolls over from 'F' to '0' and then continues counting.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The card shall set the Issuer Script Failure Indicator to 1b if one of the following error conditions occurred during card processing of an issuer script command received before or 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.

If the card supports contactless issuer update processing and the card is able to successfully validate the MAC and successfully perform the issuer script command, then the application shall set the Last Successful Issuer Update ATC Register to the value of the ATC before responding to the issuer script command.

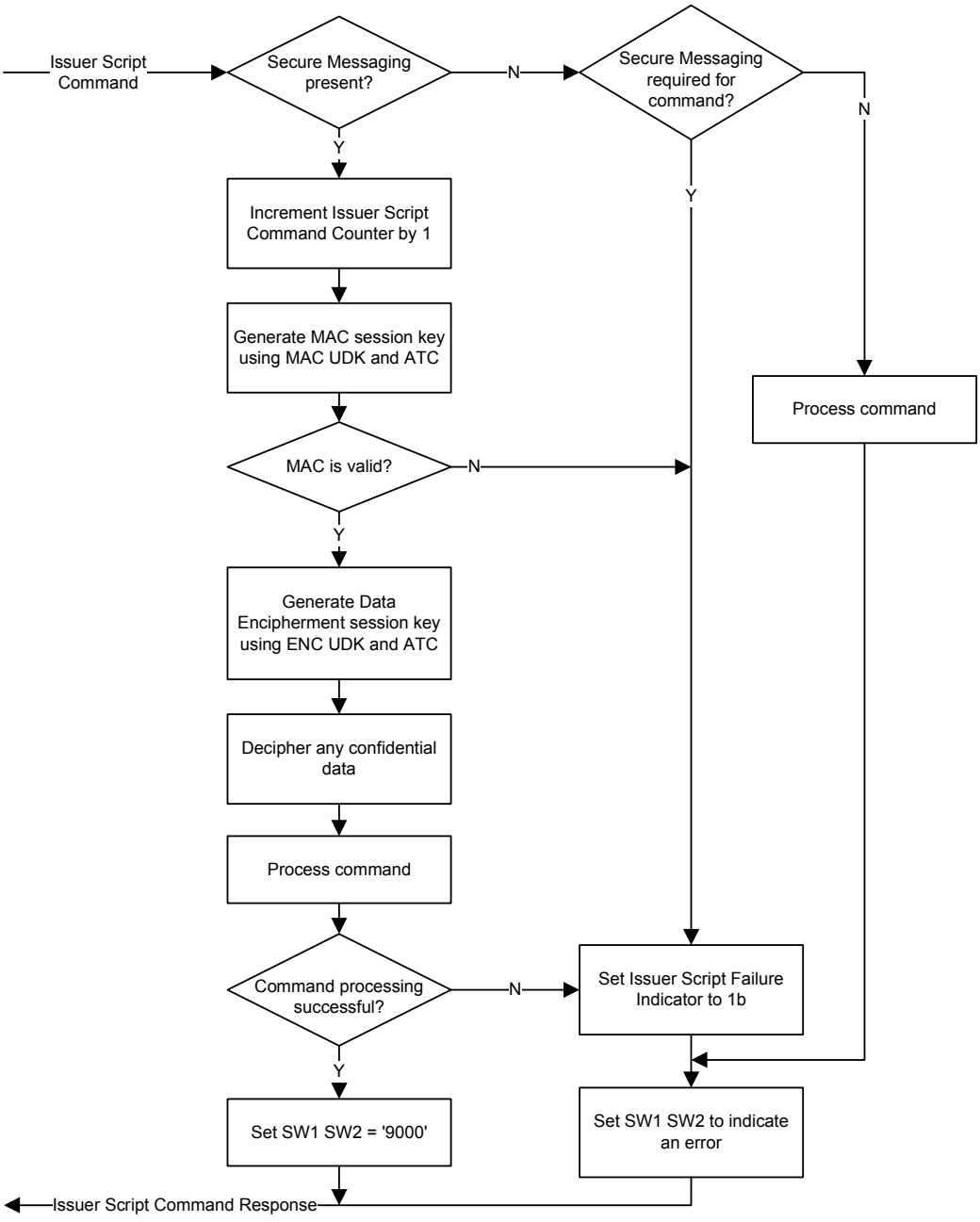
Use of Issuer Script Template 1 (for Issuer Script commands sent before the second GENERATE AC command) is not recommended unless there is a strong business need to update the card before the second GENERATE AC command.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, then Issuer-to-Card Script Processing is performed before or after the Completion process, depending on which Issuer Script Template is used.

14.8 Subsequent Related Processing

Completion (current transactions)

- The card sets the 'Number of Issuer Script Commands' bits of the CVR to the value of the Issuer Script Command Counter, using the identical bit settings before building the Issuer Application Data for the second GENERATE AC response.
- If the Issuer Script Failure Indicator is set to 1b, then the card sets the 'Issuer Script processing failed' bit of the CVR to 1b before building the Issuer Application Data for the second GENERATE AC response.

  Note: *The 'Issuer Script processing failed' bit may be set in the CVR because a script failed before the second GENERATE AC command of the current transaction, or because a script failed during a previous transaction and the indicator has not yet been reset. In order to indicate to the issuer that a script failed before the second GENERATE AC command of the current transaction, the 'Issuer Script processing failed' bit in the CVR for the second GENERATE AC response shall be set before the application determines whether to reset the Issuer Script Failure Indicator.*

- After building the Issuer Application Data for the second GENERATE AC response and before sending the second GENERATE AC response, the Issuer Script Failure Indicator is reset to 0b 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- After building the Issuer Application Data for the second GENERATE AC response and before sending the second GENERATE AC response, the Issuer Script Command Counter is reset to 0b after online transactions if the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 0b *and any* of the following conditions exist:
  - Issuer Authentication was successful
  - Issuer Authentication was optional and not performed
  - Issuer Authentication was not supported

Card Action Analysis (subsequent transactions)

During Card Action Analysis for the card's next transaction:

- The card sets the 'Number of Issuer Script Commands' bits of the CVR to value of the Issuer Script Command Counter, using the identical bit settings.
- If the Issuer Script Failure Indicator is set to 1b, then the card sets the 'Issuer Script processing failed' bit of the CVR to 1b.

  Note: *The 'Issuer Script processing failed' bit may be set in the CVR if a script failed during a previous transaction and the indicator has not yet been reset.*

Completion (subsequent transactions)

The Issuer Script Failure Indicator is reset to 0b 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

The Issuer Script Command Counter is reset to 0b after online transactions if the 'Issuer Script Command Counter is cyclic' bit of the ADA is set to 0b *and any* of the following conditions exist:

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

A VIS Data Element Tables

This appendix defines those data elements that may be used for financial transaction interchange and their mapping onto data objects. This includes all card, issuer, terminal, and acquirer data objects listed in *EMV Book 3*, Annex A, and the Visa proprietary data elements.

Note: *Although Visa does not support certain terminal-related data objects listed in* EMV Book 3*, Annex A, other payment systems may choose to support these data objects. Therefore, terminals support all terminal-related data objects listed in those specifications.*

The data elements are presented in two tables:

- Table A-1 describes each data element: name, format, tag, length, and source; whether required; description; and possible values.
- Table A-2 lists the data elements in tag sequence.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

A.1 Data Element Descriptions

Table A-1 lists the data elements used in VIS.

A.1.1 Name, Format, Template/Tag, Length and Source

The *Name* column lists the data element name, as well as the format (F), tag/template (T), length (L), and source (S).

The supported *formats* are as follows:

- n (numeric)
- cn (compressed numeric)
- b (binary or bit string)
- an (alphanumeric)
- ans (alphanumeric special)

The *tag/template* entry in this column identifies one of the following:

- the tag for a primitive data element that does not use a context-specific tag
- the template tag for a constructed data element
- the tag and template for a primitive data element that uses a context-specific tag in the range 'DF01' to 'DFFE'.

  Context-specific tags only define the corresponding data element when contained in the listed template tag. This is shown as 'DFxx' in 'BFxx', where 'DFxx' represents the context-specific data element, and 'BFxx' represents the template containing the context-specific data element..

  Note: *The meaning assigned to a context-specific tag in one template will be different from the meaning assigned to the same value context-specific tag in another template.*

  Note: *A data element that is defined with both a primitive tag and a context-specific tag within a template tag shall reference the same underlying value regardless of the tag used. The data element shall be personalizable, updateable, and accessible (for example, using the GET DATA command) using either tag.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

For applications that support Profiles functionality, the ‘x’ in tag 'aaax' identifies which instance of Data Element x is identified by the tag.

For example, the ‘x’ for 'DF1x' in 'BF56' identifies Consecutive Transaction Counter x (CTC x) – that is:

- 'DF11' in 'BF56' identifies Consecutive Transaction Counter 1 (CTC 1)
- 'DF12' in 'BF56' identifies Consecutive Transaction Counter 2 (CTC 2)
- 'DF13' in 'BF56' identifies Consecutive Transaction Counter 3 (CTC 3)
- 'DF14' in 'BF56' identifies Consecutive Transaction Counter 4 (CTC 4)

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 '0's
- A data element in format cn is left-justified and padded with trailing 'F's
- A data element in format an is left-justified and padded with trailing '0's
- A data element in format ans is left-justified and padded with trailing '0's

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.

A.1.2 Requirement

The *requirement* column lists the requirements for the presence of the data element:

- **R (Required)**—The data element shall always be present.
- **C (Conditional)**—The data element is necessary under the conditions specified.
- **O (Optional)**—The data element is optional.

A.1.3 Update Capability, Update, Retrieval, Backup, Secret

This column lists the *update capability (UC), issuer update (IU), retrieval (R), backup (B), and secret* requirements for data elements that have the card as the source. The following sections further describe the values for each of these fields.

A.1.3.1 Update Capability (UC)

The *update capability (UC)* entry in this column categorizes card-sourced data into the following classifications:

- **Unchanging**—The data element value is set before the first transaction (either by personalisation of a starting value, or to a default value) and shall not change.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- **Modifiable**—The data element value is set before the first transaction (either by personalisation of a starting value, or to a default value) and the value it contains at the end of one transaction is the value retained for use during the subsequent transaction. The value may only be modified post-issuance using an issuer script command or by setting indicators in the Card Status Updates (CSU) portion of the Issuer Authentication Data, as identified in the *issuer update (IU)* entry listed in this column.
- **Persistent**—The data element value is set before the first transaction (either by personalisation of a starting value, or to a default value) and the value it contains at the end of one transaction is the value retained for use during the subsequent transaction. The value may only be modified as part of transaction processing (for example, to indicate events that have occurred during the current transaction which may be used in processing subsequent transactions), and shall not be modified using any issuer script command nor by setting indicators in the CSU portion of the Issuer Authentication Data.
- **Dynamic**—The data element value is set before the first transaction (either by personalisation of a starting value, or to a default value) and the value it contains at the end of one transaction is the value retained for use during the subsequent transaction. The value may be modified post-issuance as a part of transaction processing, using an issuer script command, or by setting indicators in the CSU portion of the Issuer Authentication Data, as identified in the *issuer update (IU)* entry listed in this column.
- **Transient**—The data element value is reset at the beginning of a transaction, and the value set in one transaction is not retained for the subsequent transaction. The value is modified during transaction processing to indicate events that have occurred during the current transaction.

Data elements classified as *unchanging* or *persistent* may be included as part of an issuer script command to update a record or larger data element which contains the data element and is allowed to be updated. However, the value of the *unchanging* or *persistent* data element after update of the record or larger data element shall be the same as the value before the update. The application is not required to enforce this restriction, it is a requirement on the issuer script command sent to the application.

For example, the Issuer Application Data may be updated by a PUT DATA command, but the value of the CVR after the update shall be the same as the value before the update. Similarly, the record that contains the Application Expiration Date may be updated, but the value of the Application Expiration Date after the update must be the same as the value before the update.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

A.1.3.2 Issuer Update

The *issuer update (IU)* entry in this column shows whether update of the data element is allowed using an issuer update, the method (for example, the CSU in the authorization response or which issuer script command) to be used for the update, and any conditions on the support for update.

The following values are used to indicate support for update of data elements:

- **n/a**—indicates that the specification does not define a mechanism to update the data element with an issuer update (for example, the data element does not have a tag), however update of the data element is allowed.
- **N**—indicates update of the value of the data element is not allowed.

  Note: *The data element may be included as part of an update to a record or larger data element that is allowed to be updated. However, the value of this data element after update of the record or larger data element shall be the same as the value before the update. The application is not required to enforce this restriction, it is a requirement on the issuer script command sent to the application.*

- **CSU**—indicates that update of the data element is allowed using the functionality associated with the Card Status Updates data element included in the Issuer Authentication Data for CVN 18.
- **PIN CHANGE/UNBLOCK**—indicates that update of the data element is allowed using the PIN CHANGE/UNBLOCK command.
- **PUT DATA**—indicates that update of the data element is allowed using the PUT DATA command.
- **UPDATE RECORD**—indicates that update of the data element is allowed using the UPDATE RECORD command.

A.1.3.3 Retrieval

The *retrieval (R)* entry in this 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, then the data element shall be retrieved only by special devices and not by terminals during financial transactions. If the column is blank for a data element, support for retrieval of the data element is optional.

The following values are used to indicate support for retrieval of data elements:

- **n/a**—indicates that the specification does not define a mechanism to retrieve the data element (for example, the data element does not have a tag), however retrieval of the data element is allowed.
- **N**—indicates retrieval of the value of the data element shall not be allowed.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- **GENERATE AC**—indicates that the data element may be retrieved as part of the data sent in the response to the GENERATE AC command.
- **GET DATA**—indicates that retrieval of the data element is allowed using the GET DATA command.
- **GET DATA (SD)**—indicates that retrieval of the data element using the GET DATA command at special devices shall be supported for use in card approval testing, personalization validation, and investigation of potential interoperability issues.
- **GET PROCESSING OPTIONS**—indicates that the data element may be retrieved as part of the data sent in the response to the GET PROCESSING OPTIONS command.
- **INTERNAL AUTHENTICATE**—indicates that the data element may be retrieved as part of the data sent in the response to the INTERNAL AUTHENTICATE command.
- **READ RECORD**—indicates that retrieval of the data element is allowed using the READ RECORD command.
- **SELECT**—indicates that the data element may be retrieved as part of the data sent in the response to the SELECT command.

A.1.3.4 Backup

The *backup (B)* entry in this column describes the protection applicable to each *transient, dynamic, persistent* and *modifiable* data element showing whether the data element shall be backed up or defaulted to a value 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, including those classified as update capability *unchanging*). This implies the information shall not be lost nor modified in case of exceptional events.

Protection shall be ensured for the application *transient, dynamic, persistent* and *modifiable* data. The following values are used to identify forms of protection required for specific data elements:

- **Backup**—indicates that the data element value shall be backed up so that in case of an exceptional event, the data element may revert to the backed up value.
- **Backup or default to 'xxxx'** —indicates that the data element should be backed up. If not backed up, then in case of an exceptional event it shall revert to the value of the data element identified by tag 'xxxx'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- **Backup or default to (data element name)** —indicates that the data element should be backed up. If not backed up, then in case of an exceptional event it shall revert to the value of the specified data element.
- **Backup or default to (value)** —indicates that the data element should be backed up. If not backed up, then in case of an exceptional event it shall revert to the specified value.

A.1.3.5 Secret Data

Data elements identified as *Secret* in this column 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 (with the exception of the Reference PIN) shall never be updated. The Reference PIN may be updated using an Issuer Script Command such as the PIN CHANGE/UNBLOCK command with secure messaging. The following data elements are secret:

- Unique DEA Key
- Unique Data Encipherment DEA Key
- Unique MAC DEA Key
- ICC PIN Encipherment Private Key
- ICC Private Key
- Reference PIN

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (1 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Account Type F: n 2 T: '5F57' L: 1 S: Terminal	O	Indicates the type of account selected on the terminal.	n/a	'00' = Default - Unspecified '10' = Savings '20' = Cheque/debit '30' = Credit All other values RFU
Acquirer Identifier F: n 6-11 T: '9F01' L: 6 S: Terminal	O	Uniquely identifies the acquirer within each payment system. For Visa, this is the BASE Identification Number (BIN).	n/a	
Additional Terminal Capabilities F: b 40 T: '9F40' L: 5 S: Terminal	R	Indicates the data input and output capabilities of the terminal.	n/a	Byte 1 (Transaction Type Capability): bit 8: 1b = Cash bit 7: 1b = Goods bit 6: 1b = Services bit 5: 1b = Cashback bit 4: 1b = Inquiry bit 3: 1b = Transfer bit 2: 1b = Payment bit 1: 1b = Administrative *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (2 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Additional Terminal Capabilities (continued)				Byte 2 (Transaction Type Capability, cont.): bit 8: 1b = Cash deposit bits 7-1: Reserved for future use (RFU) (0000000b) ***Note:*** *A cash deposit is considered to be a transaction at an attended or unattended terminal where a cardholder deposits cash into a bank account related to an application on the card used.* Byte 3 (Terminal Data Input Capability): bit 8: 1b = Numeric keys bit 7: 1b = Alphabetic and special characters keys bit 6: 1b = Command keys bit 5: 1b = Function keys bits 4-1: RFU (0000b) Byte 4 (Terminal Data Output Capability): bit 8: 1b = Print, attendant bit 7: 1b = Print, cardholder bit 6: 1b = Display, attendant bit 5: 1b = Display, cardholder bits 4-3: RFU (00b) bit 2: 1b = Code table 10 bit 1: 1b = Code table 9 *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (3 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Additional Terminal Capabilities (continued)				Byte 5 (Terminal Data Output Capability, cont.): bit 8: 1b = Code table 8 bit 7: 1b = Code table 7 bit 6: 1b = Code table 6 bit 5: 1b = Code table 5 bit 4: 1b = Code table 4 bit 3: 1b = Code table 3 bit 2: 1b = Code table 2 bit 1: 1b = Code table 1
AIP/AFL Entry x F: b T: 'DF1x' in 'BF5A' L: Var S: Card	C If Profiles Functionality is supported	Contains the AIP, AFL Length, and AFL to be returned in the GET PROCESSING OPTIONS response for Profile x.	UC: Modifiable IU: PUT DATA R: GET PROCESSING OPTIONS	Byte 1-2: Application Interchange Profile (AIP) for Profile x Byte 3: Application File Locator Length (AFL Length) for Profile x Bytes 4-end: AFL for Profile x
AIP/AFL Entries Template F: b T: 'BF5A' L: var S: Card	C If Profiles Functionality is supported or the ability to update the AIP or AFL by issuer script is to be supported	Visa proprietary data template that contains the TLV-coded values for AIPs and AFLs.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the AIP/AFL Entries Template: 'DF1x': AIP/AFL Entry x

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (4 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Amount, Authorized (Binary) F: b 32 T: '81' L: 4 S: Terminal	not applicable	Authorized amount of the transaction (excluding adjustments). This data object is not used in this version of VIS.	n/a	
Amount, Authorized (Numeric) F: n 12 T: '9F02' L: 6 S: Terminal	R	Authorized amount of the transaction (excluding adjustments).	n/a	
Amount, Other (Binary) F: b 32 T: '9F04' L: 4 S: Terminal	not applicable	Secondary amount associated with the transaction representing a cashback amount. This data object is not used in this version of VIS.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (5 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Amount, Other (Numeric) F: n 12 T: '9F03' L: 6 S: Terminal	C If cashback supported	Secondary amount associated with the transaction representing a cashback amount.	n/a	
Amount, Reference Currency (Binary) F: b 32 T: '9F3A' L: 4 S: Terminal	not applicable	Authorized amount expressed in the reference currency. This data object is not used in this version of VIS.	n/a	
Amounts Data Template F: b T: 'BF58' L: var S: Card	C If Profiles Functionality is supported and Cumulative Total Transaction Amount card velocity checking is to be performed	Visa proprietary data template that contains the TLV-coded values for Cumulative Total Transaction Amounts and their associated Limits and Upper Limits..	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the Amounts Data Template: 'DF1x': CTTA x 'DF2x': CTTAL x 'DF3x': CTTAUL x

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (6 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Capabilities F: b 8 T: 'DF01' in 'BF5B' L: 2 S: Card	C If supported for contactless	Visa proprietary data element indicating card application capabilities.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	Byte 1: bit 8: 1b = Contactless functionality disabled bit 7: 1b = Restrict reset of Contactless functionality disabled bit bits 6-1: RFU (000000b) Byte 2: RFU ('00')
Application Cryptogram (AC) F: b 64 T: '9F26' L: 8 S: Card	R	Cryptogram returned by the ICC in the response of the GENERATE AC command (i.e., TC, ARQC, or AAC).	UC: Transient IU: N R: GENERATE AC	
Application Currency Code F: n 3 T: '9F42' L: 2 S: Card	C If Cardholder Verification Method (CVM) List has amount checks	Indicates the currency in which the amount is managed according to ISO 4217.	UC: Unchanging U: N R: READ RECORD	Shall match the value of '9F51'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (7 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Currency Code F: n 3 T: '9F51' L: 2 S: Card	C If Cumulative Total Transaction Amount or Consecutive International Transactions card velocity checking is to be performed	Visa proprietary data element indicating the currency in which the account is managed according to ISO 4217.	UC: Unchanging U: N R: GET DATA (SD)	Shall match the value of '9F42'.
Application Currency Exponent F: n 1 T: '9F44' L: 1 S: Card	O	Indicates the implied position of the decimal point from the right of the account represented according to ISO 4217.	UC: Unchanging IU: N R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (8 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) F: b 32 T: '9F52' L: 6 S: Card	C If any functionality that uses the ADA is 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, offline PIN verification checks, new card checks, and issuer script processing checks. If this data element is not present, then the application behaves as if the value is all zeroes. ***Note:*** *It is highly recommended that this data element be present for cards that support Issuer Authentication, Issuer Script commands, offline processing or dual-interface cards that support qVSDC functionality.* *- continues -*	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	If not personalized, the ADA shall be present with a value of all zero. Byte 1: bit 8: 1b = If Issuer Authentication failure, transmit next transaction online bit 7: 1b = If Issuer Authentication performed and failed, decline transaction ***Note:*** *It is highly recommended that this bit be set to 0b. Issuers are cautioned that setting this bit to 1b may cause the card to decline transactions that the issuer has approved.* bit 6: 1b = If Issuer Authentication is mandatory and no ARPC received, decline transaction ***Note:*** *It is highly recommended that this bit be set to 0b. Issuers are cautioned that setting this bit to 1b may cause the card to decline transactions that the issuer has approved.* bit 5: 1b = If transaction declined offline, create advice bit 4: 1b = If PIN Try Limit exceeded on current transaction and transaction is declined, create advice *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (9 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)		continued: Application shall accept personalization of 4 bytes of data for the ADA. In the case of ADA personalization only providing a 4 byte value, the application shall store a 6 byte value for the ADA consisting of the 4 bytes of personalized data, left justified, and padded on the right with '0000'. A PUT DATA to the ADA must send a 6 byte updated value. The application responds to a GET DATA for the ADA with a 6 byte value.		Byte 1, continued: bit 3: 1b = If transaction declined because Issuer Authentication failed or not performed, create advice bit 2: 1b = If new card, transmit transaction online bit 1: 1b = If new card, decline if unable to transmit transaction online Byte 2: bit 8: 1b = If PIN Try Limit exceeded on current transaction, block application bit 7: 1b = If PIN Try Limit exceeded on previous transaction, decline transaction bit 6: 1b = If PIN Try Limit exceeded on previous transaction, transmit transaction online bit 5: 1b = If PIN Try Limit exceeded on previous transaction, decline if unable to transmit transaction online bit 4: 1b = If Issuer Script failed on a previous transaction, transmit transaction online *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (10 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)				Byte 2, continued: bit 3: 1b = If PIN Try Limit exceeded on previous transaction, decline and block application ***Note:*** *Support for functionality associated with bit 2 and bit 1 is optional. The functionality associated with each bit may be required in some markets or for some programs.* bit 2: 1b = Do not reset CTTA during GENERATE AC. ***Note:*** *If this bit is set to 1b, CTTA is reset to zero during Issuer Script processing if PUT DATA to Cumulative Total Transaction Amount Limit is successful.* bit 1: 1b = Do not reset VLP Available Funds during GENERATE AC ***Note:*** *If this bit is set to 1b, VLP Available Funds is reset to VLP Funds Limit during Issuer Script processing when PUT DATA to VLP Funds Limit is successful instead of being reset during second GENERATE AC based on the outcome of issuer authentication.* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (11 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)				Byte 2, bit 1, continued: ***Note:*** *This bit does not restrict the resetting of VLP Available Funds during first and second GENERATE AC processing that is based on successful offline PIN verification during an approved transaction* Byte 3: ***Note:*** *Support for the functionality associated with byte 3 bits 8-6 is optional if transaction logging is supported. Implementations that do not support Transaction Logging functionality shall treat these bits as RFU (that is, ignore the setting of these bits).* ***Note:*** *If byte 3 bits 8-6 are supported as described below, the default behavior will be to include all approved transactions in the log (if present). Declined transactions will not be included unless indicated in the ADA.* ***Note:*** *If logging is supported for qVSDC transactions and the application uses ADA byte 3 bits 8-6 to control transaction logging for contact transactions, then the same ADA bits shall also be used to control logging for qVSDC transactions* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (12 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)				Byte 3, continued *(see notes for bit 8-6 on previous page)*: bit 8: 1b = Do not include offline approved transactions in the transaction log bit 7: 1b = Do not include online approved transactions in the transaction log bit 6: 1b = Include declined transactions in the transaction log bit 5: 1b = Reset VLP Available Funds to VLP Funds Limit whenever Offline PIN is successfully verified ***Note:*** *Support for the functionality associated with this bit is optional.* bit 4: 1b = Do not count declined transactions bit 3: 1b= Use Issuer Script MAC Chaining Option bit 2: 1b= Issuer Script Command Counter is cyclic ***Note:*** *If issuer scripts are supported, it is highly recommended that this bit be set to 1b so that only successful script commands are counted.* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (13 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)				Byte 3, continued: bit 1: 1b = CTCI also counts non-matching country code transactions Byte 4: ***Note:*** *Support for the functionality associated with byte 4 bits 8-6 is conditional on support for CVN 18. If the application uses CVN 10, these bits are RFU (000b).* bit 8: 1b = Use Default Update Counters in ADA if CSU is generated by a proxy bits 7-6: Default Update Counters: 00b = Do not update velocity-checking counters 01b = Set velocity-checking counters to Upper Limits 10b = Reset velocity-checking counters to Zero 11b = Add transaction to velocity-checking counters bit 5: 1b = Padding method '80' supported for IDD MACing bits 4–1: RFU (0000b) Byte 5: bits 8–5: RFU (0000b) *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (14 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)				Byte 5, continued: ***Note:*** *Support for functionality associated with byte 5 bits 4-2 is optional.* bit 4: 1b = If Offline PIN verification not performed or not successful, send transaction online bit 3: 1b = If Offline PIN verification not performed, decline if unable to transmit transaction online ***Note:*** *Issuers are strongly cautioned that setting this bit to 1b will cause the card to always decline at offline devices when PIN is not supported.* bit 2: 1b = If Offline PIN verification not successful, decline if unable to transmit transaction online ***Note:*** *Issuers are strongly cautioned that setting this bit to 1b will cause the card to always decline at offline devices when PIN is not successful, even if the PIN Try Limit has not been exceeded.* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (15 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Default Action (ADA) (continued)				Byte 5, continued: ***Note:*** *Support for the functionality associated with Byte 5 bit 1 is conditional on support of IAD Format 2 and Issuer Scripting. If the application does not support IAD Format 2 or does not support Issuer Scripts, this bit is RFU (0b).* bit 1: 1b = Secure Messaging uses EMV Session key-based derivation Byte 6: bit 8: 1b = CDCVM supported ***Note:*** *Setting this bit to 1b does not change EMV CVM List processing. Issuers should reconsider their CVM List requirements when using CDCVM.* bits 7–1: RFU (0000000b)
Application Discretionary Data F: b 8–256 T: '9F05' L: 1–32 S: Card	O	Issuer-specified data relating to the card application.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (16 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Effective Date F: n 6 YYMMDD T: '5F25' L: 3 S: Card	O	Date from which the card application may be used.	UC: Modifiable IU: UPDATE RECORD ***Note:*** *Issuers are cautioned that the update may not comply with Visa rules if the Effective Date is printed or embossed on the card plastic.* R: READ RECORD	
Application Expiration Date F: n 6 YYMMDD T: '5F24' L: 3 S: Card	R	Date after which the card application expires.	UC: Unchanging IU: N R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (17 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application File Locator (AFL) F: var. T: '94' L: var. up to 252 S: Card	R	Indicates the location (SFI, range of records) of the AEFs related to a given application.	UC: Modifiable IU: PUT DATA ***Note:*** *PUT DATA to this data element updates the only AFL used for transactions over the contact interface. If multiple AFLs are supported for contact chip transactions, PUT DATA to AIP/AFL Entries shall be used to change the values used for the AFL.* R: GET PROCESSING OPTIONS	For each file to be read, the Application File Locator contains the following four bytes: Byte 1: bits 8–4 = SFI bits 3–1 = 000b 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)
Application Identifier (AID) F: b 40–128 T: '4F' L: 5–16 S: Card	C If Directory method of Application Selection (PSE) is supported	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)	UC: Unchanging IU: N R: READ RECORD	The Visa RID is 'A000000003'. The global Visa AIDs are: 'A0000000031010' Visa Debit or Credit 'A0000000032010' Visa Electron 'A0000000033010' Interlink 'A0000000038010' PLUS

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (18 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Identifier (AID) F: b 40-128 T: '9F06' L: 5-16 S: Terminal	R	Identifies the application as described in ISO/IEC 7816-5.	n/a	
Application Interchange Profile (AIP) F: b 16 T: '82' L: 2 S: Card	R	Indicates the capabilities of the card to support specific functions in the application.	UC: Modifiable IU: PUT DATA ***Note:*** *PUT DATA to this data element updates the only AIP used for transactions over the contact interface. If multiple AIPs are supported for contact chip transactions(for example, for Profiles Functionality), PUT DATA to AIP/AFL Entries shall be used to change the values used for the AFL.* R: GET PROCESSING OPTIONS	Byte 1: bit 8: RFU (0b) bit 7: 1b = SDA is supported ***Note:*** *Bit 7 shall be set to 0b.* bit 6: 1b = DDA is supported bit 5: 1b = Cardholder verification is supported ***Note:*** *Bit 5 shall be set to 1b.* bit 4: 1b = Terminal Risk Management is to be performed ***Note:*** *Bit 4 shall be set to 1b.* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (19 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Interchange Profile (AIP) (continued)				Byte 1, continued: bit 3: 1b = Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command ***Note:*** *Issuers that support Issuer Authentication for CVN 18 shall set bit 3 to 0b.Issuers that support Issuer Authentication for CVN 10 may set bit 3 to 0b (the application will perform Issuer Authentication during GENERATE AC command processing instead of using the EXTERNAL AUTHENTICATE command).* bit 2: RFU (0b) bit 1: 1b = CDA is supported Byte 2: bit 8: Not used for VIS bits 7-1: RFU (0000000b)
Application Internal Data Template F: b T: 'BF5B' L: var. S: Card	C If Profiles Functionality is supported or Application Capabilities is supported for contactless	Visa proprietary data template that contains Visa Proprietary context-specific tags for application internal data.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the Application Internal Data Template: 'DF01': Application Capabilities 'DF02': Profile Selection File Entry

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (20 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Label F: ans 1–16 * T: '50' L: 1–16 * (special characters limited to spaces) S: Card	R	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.	UC: Unchanging IU: N R: READ RECORD, SELECT	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" ***Note:*** *"Visa" may be eliminated for Electron Products if the required Application Label would exceed 16 bytes length. Regional permission is required.* Interlink Shall include "Interlink". For example, "Interlink" or "Visa Interlink" PLUS Shall include "PLUS". For example, "PLUS" or "PLUS ATM"

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (21 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Preferred Name F: ans 1–16 T: '9F12' L: 1–16 S: Card	O	Preferred mnemonic associated with the AID. Terminal displays during application selection if the terminal supports any character set designated in the Issuer Code Table Index.	UC: Unchanging IU: N R: READ RECORD, SELECT	
Application Primary Account Number (PAN) F: var. up to cn 19 T: '5A' L: var. up to 10 S: Card	R	Valid cardholder account number.	UC: Unchanging IU: N R: READ RECORD	
Application Primary Account Number (PAN) Sequence Number F: n 2 T: '5F34' L: 1 S: Card	O	Identifies and differentiates card applications with the same PAN.	UC: Unchanging IU: N R: READ RECORD	***Note:*** *Although this field is optional in the card, if it is present in the card it is sent in online messages. If it is not sent in online messages, the value is assumed to be '00' for key derivations.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (22 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Priority Indicator F: b 8 T: '87' L: 1 S: Card	C If multiple payment applications on card	Indicates the priority of a given application or group of applications in a directory.	UC: Unchanging IU: N R: READ RECORD, SELECT	bit 8 = 1b: Application shall not be selected without confirmation of cardholder 0b: Application may be selected without confirmation of cardholder bits 7–5: RFU (000b) bits 4–1: 0000b= 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 S: Card	not applicable	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.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (23 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Reference Currency Exponent F: n 1 T: '9F43' L: 1–4 S: Card	not applicable	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.	n/a	
Application Selection Indicator F: – T: – L: – S: Terminal	R	Indicates whether the associated AID in the terminal shall match the AID in the card exactly including the length of the AID, or only up to the length of the AID in the terminal. There is only one Application Selection Indicator per AID in the terminal.	n/a	Format and content are at the discretion of the terminal vendor. For Visa applications, shall be set to indicate support for partial name selection.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (24 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Selection Registered Proprietary Data (ASRPD) F: b T: '9F0A' L: var. S: Card	O	Market-proprietary data that may be required by local regulatory authority to offer specific services based on this information, as defined in [EMV ASRPD]. The Application Selection Registered Proprietary Data may be returned by the card during Application Selection - that is, it may be present in one or both of the following: • In the Directory Discretionary data (tag '73') within any ADF Directory Entry • In the FCI Issuer Directory Discretionary Data (tag 'BF0C') within the FCI of any ADF. *Use of the Application Selection Registered Proprietary Data by the terminal is optional and proprietary, and is outside the scope of this specification*.	UC: Unchanging IU: N R: READ RECORD, SELECT	The value field of the Application Selection Registered Proprietary Data follows the following format: ID1, L1, V1, ID2, L2, V2,… Where • IDn is a two byte Proprietary Data Identifier, registered by EMVCo. IDs have no structure (they are not BER-TLV tags), and may be in any order within the ASRPD. • Ln is the length of the value field coded in 1 byte (0 to 255). • Vn is the value field. Its content is proprietary and format is out of scope of EMVCo. See [EMV ASRPD] for additional information.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (25 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Template F: b T: '61' L: var. up to 252 S: Card	C If PSE present	Template containing one or more data objects relevant to an application directory entry according to ISO/IEC 7816-5.	UC: Unchanging IU: N R: SELECT	
Application Transaction Counter (ATC) F: b 16 T: '9F36' L: 2 S: Card	R	Counter of the number of transactions processed since personalization. Maintained by the application in the card.	UC: Persistent IU: N R: GET DATA (if terminal velocity checking is to be performed) B: Backup	Initial value is zero unless optionally personalized to an initial starting value. Incremented by 1 during Initiate Application Processing each time a transaction is performed. Never reset. If the ATC reaches its maximum value, then the application shall be permanently blocked as described in section 4.4.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (26 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Usage Control F: b 16 T: '9F07' L: 2 S: Card	O	Indicates issuer-specified restrictions on the geographic usage and services allowed for the card application.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Byte 1: bit 8: 1b = Valid for domestic cash transactions bit 7: 1b = Valid for international cash transactions bit 6: 1b = Valid for domestic goods bit 5: 1b = Valid for international goods bit 4: 1b = Valid for domestic services bit 3: 1b = Valid for international services bit 2: 1b = Valid at ATMs bit 1: 1b = Valid at terminals other than ATMs Byte 2: bit 8: 1b = Domestic cashback allowed bit 7: 1b = International cashback allowed bits 6–1: RFU (000000b) 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (27 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Application Version Number F: b 16 T: '9F08' L: 2 S: Card	R	Version number assigned by the payment system for the application.	UC: Unchanging IU: N R: READ RECORD	The Application Version Number is the version, release, and modification number in binary of VIS supported by the card. • For cards supporting VIS 1.6, the value is 160 ('00A0').
Application Version Number F: b 16 T: '9F09' L: 2 S: Terminal	R	Version number assigned by the payment system for the application.	n/a	The Application Version Number is the version, release, and modification number in binary of VIS supported by the terminal.
Authorization Code F: ans 6 * T: '89' L: 6 * (special characters limited to spaces) S: Issuer	From issuer. Not passed to card	Nonzero value generated by the issuer for an approved transaction.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (28 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Authorization Response Code F: an 2 T: '8A' L: 2 S: Issuer/Terminal	R Passed from issuer through terminal Generated by the terminal if unable to go online Set by the terminal during Terminal Action Analysis	Indicates the disposition of the transaction received from issuer for online authorizations for transactions using CVN 10. If the terminal is unable to go online, the terminal generates EMV-specified values. During Terminal Action Analysis, the Authorization Response Code is set based on the terminal's decision.	n/a	Codes generated by the issuer are as indicated in ISO 8583:1987. The following codes are generated by the terminal for transactions that were unable to go online and are used by the card in Completion Processing: Y3 = Unable to go online (offline approved) Z3 = Unable to go online (offline declined) The following codes are Set by the terminal during Terminal Action Analysis: Y1 = Offline approved Z1 = Offline declined ***Note:*** *Instead of Authorization Response Code, the P1 parameter of the first GENERATE AC commands indicates the type of cryptogram the terminal is requesting.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (29 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Authorization Response Cryptogram (ARPC) F: b T: Part of '91' for CVN 18 L: 8 (for CVN 10) 4 (for CVN 18) S: Issuer/Terminal	O Passed from issuer through terminal	Cryptogram returned by the issuer (if Issuer Authentication is supported) in the online response, and used by the card to verify that the response came from the issuer.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (30 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Available Offline Spending Amount (AOSA) F: n 12 T: '9F5D' L: 6 S: Card	O	Visa proprietary data element indicating the remaining amount available to be spent offline.	UC: Transient IU: N R: GENERATE AC (if included in the Issuer Discretionary Data Option supported as described in Appendix J)	If the application does not also support qVSDC functionality, this amount is obtained by subtracting the Cumulative Total Transaction Amount (CTTA) from the Cumulative Total Transaction Amount Limit (CTTAL). If the application also supports qVSDC functionality and the Card Additional Processes (CAP) data element is present, the Available Offline Spending Amount shall be calculated as follows: • If the 'Low Value Check supported' bit of the CAP is set to 1b, AOSA = VLP Available Funds. • If the 'Low Value AND CTTA Check supported' bit of the CAP is set to 1b: – If Cumulative Total Transaction Amount Upper Limit (CTTAUL) is present, AOSA = CTTAUL minus CTTA – If CTTAUL is not present, AOSA = CTTAL minus CTTA • If the 'Low Value Check supported' bit of the CAP is set to 0b and the 'Low Value AND CTTA Check supported' bit of the CAP is set to 0b, AOSA = CTTAL minus CTTA. • If the calculation of the value for AOSA results in a negative value, the AOSA value shall be set to zero.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (31 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Bank Identifier Code (BIC) F: var. T: '5F54' L: 8 or 11 S: Card	O	Uniquely identifies a bank as defined in ISO 9362. In template 'BF0C' or '73'.	UC: Unchanging IU: N R: READ RECORD, SELECT	
Bit Mask F: b 8 T: – L: Block Length S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Used to mask the extracted data to allow only selected portions of the extracted data to be used as input for processing the Profile Selection Entry (for example, the comparison may be made with only a few bits of a byte). The first Comparison Block is always considered a Bit Mask. The Bit Mask is only used on data extracted from the Profile Selection Input Data (resulting in "masked extracted data"). See section E.1.3 for details on the use of the Bit Mask for each Check Type.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Each bit whose value is to be used in the comparison shall be set to 1b. Each bit whose value is not used in the comparison shall be set to 0b. ***Note:*** *The Bit Mask must always be personalized, even for Check Types for which it is not used. A value of all 'F's for the Bit Mask is recommended for Check Types that do not use the Bit Mask in the comparison (e.g., '2x', '3x', '4x', and '52').*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (32 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Block Length F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Contains the length of the portion of Profile Selection Input Data that is used as extracted data input for processing a single Profile Selection Entry in the Profile Selection process. It is also the length of each Comparison Value contained in the same Profile Selection Entry.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	For Check Types that use the value of an application internal data element (such as a counter) instead of using Profile Selection Input Data (for example, Check Types '2x', '3x', '4x', or '52'), Block Length shall be the length of the application internal data element.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (33 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Additional Processes F: b 32 T: '9F68' L: 4 S: Card	C If supported for contactless	Indicates card processing requirements and preferences for the contactless application.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Byte 1 bit 8: 1b = Low Value Check supported bit 7: 1b = Low Value AND CTTA Check supported bit 6: Not used for VIS bit 5: RFU (0b) bits 4-1: Not used for VIS Byte 2 bits 8-7: Not used for VIS bit 6: RFU (0b) bit 5: Contactless Issuer Update Processing supported bits 4-2: RFU (000b) bit 1: Not used for VIS Byte 3 bits 8-7: Not used for VIS bit 6: RFU (0b) bit 5: Not used for VIS bits 4-1: RFU (0000b) Byte 4 bit 8: Not used for VIS bits 7-1 RFU (0000000b)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (34 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Risk Management Data Object List 1 (CDOL1) F: b T: '8C' L: var. up to 252 S: Card	R	List of data objects (tags and lengths) to be passed to the card application with the first GENERATE AC command.	UC: Unchanging IU: N R: READ RECORD	
Card Risk Management Data Object List 2 (CDOL2) F: b T: '8D' L: var. up to 252 S: Card	R	List of data objects (tags and lengths) to be passed to the card application with the second GENERATE AC command.	UC: Unchanging IU: N R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (35 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Status Update (CSU) F: b 32 T: – L: 4 S: Issuer/Terminal	O Passed from issuer through terminal	Indicates the disposition of the transaction and requested updates to the card, received from the issuer for online authorizations. The CSU is only used if Issuer Authentication is performed and passes.	n/a	Byte 1: bit 8: 1b = Proprietary Authentication Data included bits 7-5: RFU (000b) bits 4-1: PIN Try Counter Byte 2: bit 8: 1b = Issuer approves online transaction bit 7: 1b = Card block bit 6: 1b = Application block bit 5: 1b = Update PIN Try Counter bit 4: 1b = Set Go Online on Next Transaction bit 3: 1b = CSU generated by proxy for the issuer ***Note:*** *When Byte 2 bit 3 is set to 1b, issuers can use the ADA (instead of the following two bits) to control what processing occurs for counter updates.* bits 2–1: Update Counters 00b = Do not update velocity-checking counters 01b = Set velocity-checking counters to Upper Limits 10b = Reset velocity-checking counters to Zero 11b = Add transaction to velocity-checking counters Byte 3: RFU ('00') Byte 4: Issuer-Discretionary (or '00')

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (36 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Verification Results (CVR) F: b 32 T: Part of '9F10' L: 4 (for IAD Format 0/1/3, 5 for IAD Format 2) S: Card	R	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. This version of VIS supports the following CVR formats: • CVR for IAD Format 0/1/3 • CVR for IAD Format 2 as defined in Appendix F, Issuer Application Data and Card Verification Results Formats	UC: Transient IU: N R: GENERATE AC	Byte 1: Length indicator ('03') for IAD Format 0/1/3, RFU ('00') for IAD Format 2 Byte 2: bits 8–7: 00b = AAC returned in second GENERATE AC 01b = TC returned in second GENERATE AC 10b = Second GENERATE AC not requested 11b = RFU bits 6–5: 00b = AAC returned in first GENERATE AC 01b = TC returned in first GENERATE AC 10b = ARQC returned in first GENERATE AC 11b = RFU ***Note:*** *If only one GENERATE AC command is issued for a transaction, then 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.* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (37 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Verification Results (CVR) (continued)				Byte 2, continued: bit 4: 1b = Issuer Authentication performed and failed bit 3: 1b = Offline PIN verification performed bit 2: 1b = Offline PIN verification failed bit 1: 1b = Unable to go online Byte 3: bit 8: 1b = Last online transaction not completed bit 7: 1b = PIN Try Limit exceeded bit 6: 1b = Exceeded velocity checking counters bit 5: 1b = New card bit 4: 1b = Issuer Authentication failure on last online transaction bit 3: 1b = Issuer Authentication not performed after online authorization bit 2: 1b = Application blocked by card because PIN Try Limit exceeded bit 1: 1b = Offline static data authentication failed on last transaction and transaction declined offline *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (38 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Verification Results (CVR) (continued)				Byte 4: bits 8–5: Number of Issuer Script Commands bit 4: 1b = Issuer Script processing failed bit 3: 1b = Offline dynamic data authentication failed on last transaction and transaction declined offline bit 2: 1b = Offline dynamic data authentication performed bit 1: 1b = PIN verification command not received for a PIN-Expecting card Byte 5 (for IAD Format 2): bits 8–3: RFU (000000b) bit 2: 1b = CDCVM Successfully Performed ***Note:*** *This bit is always set if the 'CDCVM Supported' bit of the ADA is 1b.* bit 1: 1b = Secure Messaging uses EMV Session key-based derivation.

- continues -

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (39 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Card Verification Results (CVR) (continued)				Byte 5 (for IAD Format 2), continued: ***Note:*** *If the application supports Secure Messaging with IAD Format 2, a value of 0b for Byte 5 bit 1 indicates that Secure Messaging uses XOR Session Key-based derivation. If the application does not support Secure Messaging, this bit is RFU (0b).* The following Bytes are reset to all zeros during Initiate Application Processing, and are set during Offline Data Authentication, Cardholder Verification, Card Action Analysis, Completion, and issuer script processing: • Bytes 2–4 for IAD Format 0/1/3 • Bytes 1–5 for IAD Format 2

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (40 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cardholder Name F: ans 2–26 T: '5F20' L: 2–26 S: Card	R	Indicates cardholder name according to ISO/IEC 7813	UC: Unchanging IU: N R: READ RECORD	***Note:*** *Issuers are cautioned that a very small number of old terminals may decline transactions if the tag for Cardholder Name is not present in a record listed in the AFL.* ***Note:*** *On dual-interface cards, the Cardholder Name might be personalized with a generic value (such as VISA CARDHOLDER) instead of the individual cardholder's name.* ***Note:*** *Only the following characters should be used in Cardholder Name:* • alphanumerics: "A"-"Z", "0"-"9" • hyphen: "-" • period: "." • forward slash: "/" (used as a delimiter) *The following characters may be used, but are not recommended:* • dollar sign: "$" • parenthese: "(", ")" *Use of other characters is not allowed (or has restricted use) for the Cardholder Name in the magnetic stripe, so should not be used for Cardholder Name in the chip data.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (41 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cardholder Name—Extended F: ans 27–45 T: '9F0B' L: 27–45 S: Card	O	Indicates the whole cardholder name when greater than 26 characters, using the same coding convention as in ISO/IEC 7813.	UC: Unchanging IU: N R: READ RECORD	
Cardholder Verification Method (CVM) List F: b T: '8E' L: var. up to 252 S: Card	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).*	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Bytes 1–4: Amount (“X”) (binary) Bytes 5–8: Amount (“Y”) (binary) Byte 9 (CVM Code): bit 8: 0b = Only value for methods conforming to this specification bit 7: 1b = Apply succeeding CVM field if this CVM is unsuccessful 0b = Fail cardholder verification if this CVM is unsuccessful *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (42 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cardholder Verification Method (CVM) List (continued)				Byte 9 (CVM Code), continued: bits 6–1 (CVM Type): 000000b = Fail CVM processing 000001b = Plaintext PIN verification performed by ICC 000010b = Enciphered PIN verified online 000011b = Plaintext PIN verification performed by ICC and signature (paper) 000100b = Enciphered PIN verification performed by ICC 000101b = Enciphered PIN verification performed by ICC and signature (paper) 011110b = Signature (paper) 011111b = No CVM required 000110b–011101b = RFU by EMV 100000b–101111b = RFU by individual payment systems 110000b–111110b = RFU by issuer 111111b = RFU *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (43 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cardholder Verification Method (CVM) List (continued)				Byte 10 (CVM Condition Code): '00' = Always '01' = If unattended cash ***Note:*** *Issuers should consider that older devices may interpret this code to mean "If cash or cashback", which includes unattended cash, manual cash, and purchase with cashback.* ***Note:*** *Balance enquiries and PIN change transactions that are processed through the Visa PIN Management Service are included in the "If unattended cash" code.* '02' = If not unattended cash and not manual cash and not purchase with cashback '03' = If terminal supports the CVM '04' = If manual cash '05' = If purchase with cashback '06' = If transaction is in Application Currency Code and is 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 *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (44 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cardholder Verification Method (CVM) List (continued)				Byte 10 (CVM Condition Code), continues: '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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (45 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cardholder Verification Method (CVM) Results F: b 24 T: '9F34' L: 3 S: Terminal	R	Indicates the results of the last CVM performed.	n/a	Byte 1 (CVM Performed): Last CVM of the CVM List actually performed by the terminal. Coded as a 1-byte CVM Code (as defined in the CVM List) ('3F' if no CVM is performed). Byte 2 (CVM Condition): Coded as a 1-byte CVM Condition Code (as defined in the CVM List) Byte 3 (CVM Result): Result of the (last) CVM performed as know by the terminal: '00' = Unknown (for example, for signature) '01' = Failed (for example, for offline PIN) '02' = Successful (for example, for offline PIN)
Certificate Authority Public Key F: b T: – L: – S: Terminal	C If SDA, DDA, CDA, or Offline Enciphered PIN supported	Payment system public key used for offline static or dynamic data authentication.	n/a	Value generated by Visa and loaded to terminal by acquirer. Up to six Visa public keys are supported.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (46 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Certificate Authority Public Key Check Sum F: b T: – L: 20 S: Terminal	C If SDA, DDA, CDA, or Offline Enciphered PIN supported	A check value calculated on the concatenation of all parts of the Certificate Authority Public Key (RID, Certificate Authority Public Key Index, Certificate Authority Public Key Modulus, Certificate Authority Public Key Exponent) using SHA-1.	n/a	
Certificate Authority Public Key Exponent F: b T: – L: 1 or 3 S: Terminal	C If SDA, DDA, CDA, or Offline Enciphered PIN supported	Value of the exponent part of the Certificate Authority Public Key.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (47 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Certificate Authority Public Key Index (PKI) F: b 8 T: '8F' L: 1 S: Card	C If SDA, DDA, CDA, 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.	UC: Unchanging IU: N R: READ RECORD	Values assigned by Visa.
Certificate Authority Public Key Index (PKI) F: b 8 T: '9F22' L: 1 S: Terminal	C If SDA, DDA, CDA, 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.	n/a	Values assigned by Visa.
Certificate Authority Public Key Modulus F: b T: – L: NCA (up to 248) S: Terminal	C If SDA, DDA, CDA, or Offline Enciphered PIN supported	Value of the modulus part of the Certificate Authority Public Key.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (48 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Check Type F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Identifies the type of test to be performed using masked data extracted from the Profile Selection Input Data, internal application data, or the Comparison Value(s) in the Profile Selection Entry, as determined by the Check Type. The result of the test determines the action to be taken by the application to continue Profile Selection processing. If the result is True, take the Positive Action. If the result is False, take the Negative Action).	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	'00' = Input Matches Comparison Value(s) '02' = Input Greater Than Comparison Value 1 '1x' = Input Greater Than CTTA x Funds '2x' = CTC x Greater Than Comparison Value 1 '3x' = CTCI x Greater Than Comparison Value 1 '4x' = CTCIC x Greater Than Comparison Value 1 '51' = Input Greater Than VLP Available Funds '52' = CLTC Funds Greater Than Comparison Value 1

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (49 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Chip Condition Code F: n 1 T: – L: – S: Terminal	C Mag stripe initiated from an IC reading terminal	V.I.P./BASE II data element indicating for a magnetic stripe initiated transaction whether the previous transaction at the terminal was a successful IC read.	n/a	
Command Template F: b T: '83' L: var. S: Terminal	R	Identifies the data field of a command message.	n/a	
Comparison Blocks F: b 8 T: – L: var. S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Contains the concatenation of the Bit Mask and one or more Comparison Values in a single Profile Selection Entry. ***Note:*** *The Bit Mask and at least Comparison Value 1 must always be personalized, even for Check Types for which they are not used.*	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Contains: • Bit Mask • Comparison Value 1 • ... • Comparison Value (n-1) where n = Number of Blocks. The length of Comparison Blocks = (Block Length) x (Number of Blocks)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (50 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Comparison Value x F: b 8 T: – L: Block Length S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. See section E.1.3 for details on the use of Comparison Value(s) for each Check Type. x ranges from 1 to (Number of Blocks minus 1). ***Note:*** *At least Comparison Value 1 must always be personalized, even for Check Types for which it is not used (e.g., '1x' and '51').*	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	
Consecutive Transaction Counter (CTC) F: b 8 T: 'DF11' in 'BF56' L: 1 S: Card	C If Consecutive Transaction card velocity checking is to be performed	Visa proprietary data element specifying the number of consecutive offline transactions that have occurred for that card application since the counter was reset.	UC: Dynamic IU: PUT DATA or CSU R: GET DATA (SD) B: Backup or default to '9F58' or 'DF21' in 'BF56'	Initialized to zero unless optionally personalized to a starting value. Incremented by 1 each time a transaction is approved (and optionally if declined) offline. Reset to zero if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (51 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction Counter International (CTCI) F: b 8 T: 'DF11' in 'BF57' L: 1 S: Card	C If Consecutive International Transactions card velocity checking is to be performed	Visa proprietary data element specifying the number of consecutive offline international transactions (those transactions not in the card's designated currency and if currency conversion is supported also not in a designated alternate currency, or optionally transactions not in the issuer's country) that have occurred for that card application since thecounter was reset.	UC: Dynamic IU: PUT DATA or CSU R: GET DATA (SD) B: Backup or default to '9F53' or 'DF21' in 'BF57'	Initialized to zero unless optionally personalized to a starting value. Incremented by 1 each time an international transaction is approved (and optionally if declined) offline. Reset to zero if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.
Consecutive Transaction Counter International Country (CTCIC) F: b 8 T: 'DF51' in 'BF57' L: 1 S: Card	C If Consecutive International Country Transactions card velocity checking is 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 counter was reset.	UC: Dynamic IU: PUT DATA or CSU R: GET DATA (SD) B: Backup or default to '9F72' or 'DF61' in 'BF57'	Initialized to zero unless optionally personalized to a starting value. Incremented by 1 each time an international transaction is approved (and optionally if declined) offline. Reset to zero if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (52 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction Counter International Country Limit (CTCICL) F: b 8 T: '9F72' or 'DF61' in 'BF57' L: 1 S: Card	C If Consecutive International Country Transactions Lower Limit card velocity checking is to be 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.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.
Consecutive Transaction Counter International Limit (CTCIL) F: b 8 T: '9F53' or 'DF21' in 'BF57' L: 1 S: Card	C If Consecutive International Transactions Lower Limit card velocity checking is to be performed	Visa proprietary data element specifying the maximum number of the consecutive offline international transactions (those transaction not in the card's designated currency and if currency conversion is supported also not in a designated alternate currency, or optionally transactions not in the issuer's country) allowed for that card application before a transaction is requested to go online.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (53 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction International Upper Limit (CTIUL) F: b 8 T: '9F5E' or 'DF31' in 'BF57' L: 1 S: Card	C If Consecutive International Transactions Upper Limit or Consecutive International Country Transactions Upper Limit card velocity checking is to be performed	Visa proprietary data element indicating issuer-specified preference for the maximum number of consecutive offline international transactions allowed before the transaction is declined offline if it cannot be processed online. This same Upper Limit is used regardless of whether international is determined based on currency or country (CTIUL is used for both CTCI and CTCIC).	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. ***Note:*** *It is highly recommended that the Consecutive Transaction International Upper Limit be personalized if the Consecutive Transaction Counter International Limit or Consecutive Transaction Counter International Country Limit is personalized.*
Consecutive Transaction Counter Limit (CTCL) F: b 8 T: '9F58' or 'DF21' in BF56' L: 1 S: Card	C If Consecutive Transaction Lower Limit card velocity checking is to be performed	Visa proprietary data element indicating issuer-specified preference for maximum number of consecutive offline transactions allowed for the application in a terminal with online capability.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. *Formerly Lower Consecutive Offline Limit (Card).*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (54 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction Counter Upper Limit (CTCUL) F: b 8 T: '9F59' or 'DF31' in BF56' L: 1 S: Card	C If Consecutive Transactions Upper Limit card velocity checking is to be performed by the card	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.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. *Formerly Upper Consecutive Offline Limit (Card).* ***Note:** It is highly recommended that the Consecutive Transaction Counter Upper Limit be personalized if the Consecutive Transaction Counter Limit is personalized.*
Consecutive Transaction Counter x (CTC x) F: b 8 T: 'DF1x' in 'BF56' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive Transactions card velocity checking is to be performed	If multiple CTCs are supported for Profiles , then the 'x' in the tag identifies which CTC is identified by the tag (e.g. CTC 1 is 'DF11' in 'BF56', CTC 4 is 'DF14' in 'BF56').	UC: Dynamic IU: PUT DATA or CSU R: GET DATA (SD) B: Backup or default to 'DF2x' in 'BF56'	Initialized to zero unless optionally personalized to a starting value. If counting is allowed for the Profile, incremented by 1 each time a transaction is approved (and optionally if declined) offline. If reset is allowed for the Profile, reset to 0 if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (55 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction Counter International Country x (CTCIC x) F: b 8 T: 'DF5x' in 'BF57' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive International Country Transactions card velocity checking is to be performed	If multiple CTCICs are supported for Profiles, then the 'x' in the tag identifies which CTCIC is identified by the tag (e.g. CTCIC 1 is 'DF51' in 'BF57', CTCIC 4 is 'DF54' in 'BF57').	UC: Dynamic IU: PUT DATA or CSU R: GET DATA (SD) B: Backup or default to '9F72' or 'DF6x' in 'BF57'	Initialized to zero unless optionally personalized to a starting value. If counting is allowed for the Profile, incremented by 1 each time an international transaction is approved (and optionally if declined) offline. If reset is allowed for the Profile, reset to 0 if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.
Consecutive Transaction Counter International Country Limit x (CTCICL x) F: b 8 T: 'DF6x' in 'BF57' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive International Country Transactions Lower Limit card velocity checking is to be performed	If multiple CTCICLs are supported for Profiles, then the 'x' in the tag identifies which CTCICL x is identified by the tag (e.g. CTCICL 1 is 'DF61' in 'BF57', CTCICL 4 is 'DF64' in 'BF57').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (56 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction Counter International x (CTCI x) F: b 8 T: 'DF1x' in 'BF57' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive International Transactions card velocity checking is to be performed	If multiple CTCIs are supported for Profiles , then the 'x' in the tag identifies which CTCI is identified by the tag (e.g. CTCI 1 is 'DF11' in 'BF57', CTCI 4 is 'DF14' in 'BF57').	UC: Dynamic IU: PUT DATA or CSU R: GET DATA (SD) B: Backup or default to 'DF2x' in 'BF57'	Initialized to zero unless optionally personalized to a starting value. If counting is allowed for the Profile, incremented by 1 each time an international transaction is approved (and optionally if declined) offline. If reset is allowed for the Profile, reset to 0 if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met.
Consecutive Transaction Counter International Limit (CTCIL x) F: b 8 T: 'DF2x' in 'BF57' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive International Transactions Lower Limit card velocity checking is to be performed	If multiple CTCILs are supported for Profiles , then the 'x' in the tag identifies which CTCIL x is identified by the tag (e.g. CTCIL 1 is 'DF21' in 'BF57', CTCIL 4 is 'DF24' in 'BF57').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (57 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction International Upper Limit x (CTIUL x) F: b 8 T: 'DF3x' in 'BF57' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive International Transactions Upper Limit or Consecutive International Country Transactions Upper Limit card velocity checking is to be performed	If multiple CTIULs are supported for Profiles , then the 'x' in the tag identifies which CTIUL x is identified by the tag (e.g. CTIUL 1 is 'DF31' in 'BF57', CTIUL 4 is 'DF34' in 'BF57').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. ***Note:*** *It is highly recommended that the Consecutive Transaction International Upper Limit x be personalized if the associated Consecutive Transaction Counter International Limit x or Consecutive Transaction Counter International Country Limit x is personalized.*
Consecutive Transaction Counter Limit x (CTCL x) F: b 8 T: 'DF2x' in BF56' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive Transactions Lower Limit card velocity checking is to be performed	If multiple CTCLs are supported for Profiles, then the 'x' in the tag identifies which CTCL x is identified by the tag (e.g. CTCL 1 is 'DF21' in 'BF56', CTCL 4 is 'DF24' in 'BF56').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (58 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Consecutive Transaction Counter Upper Limit x (CTCUL x) F: b 8 T: 'DF3x' in BF56' L: 1 S: Card	C If Profiles Functionality is supported and Consecutive Transactions Upper Limit card velocity check is to be performed	If multiple CTCULs are supported for Profiles, then the 'x' in the tag identifies which CTCUL x is identified by the tag (e.g. CTCUL 1 is 'DF31' in 'BF56', CTCUL 4 is 'DF34' in 'BF56').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. ***Note:*** *It is highly recommended that the Consecutive Transaction Counter Upper Limit x be personalized if the associated Consecutive Transaction Counter Limit x is personalized.*
Contactless Counters Data Template F: b T: 'BF55' L: var S: Card	C If contactless card velocity checking is to be performed	Visa proprietary data template that contains the TLV-coded values for the contactless counters and their associated Limits, Upper Limits, and thresholds.	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the Contactless Counters Data Template: 'DF11': CLTC 'DF21': CLTCLL 'DF31': CLTCUL 'DF41': VLP Single Transaction Limit 'DF51': VLP Available Funds 'DF61': VLP Reset Threshold 'DF71': VLP Funds Limit

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (59 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Contactless Transaction Counter (CLTC) F: b 8 T: 'DF11' in 'BF55' L: 1 S: Card	C If supported for contactless card velocity checking	Visa proprietary data element specifying the number of consecutive contactless transactions that have occurred on a dual-interface card since the counter was reset. Reset can occur on contact transactions.	UC: Dynamic IU: PUT DATA, CSU R: GET DATA (SD) B: Backup or default to 'DF21' in 'BF55'	Initialized to zero unless optionally personalized to a starting value. Configurable to follow one of the three following rules: • Incremented by 1 each time only a qVSDC offline transaction is approved. • Incremented by 1 each time only a qVSDC online transaction occurs. • Incremented by 1 each time either a qVSDC offline transaction approved or online transaction occurs. Reset to 0 if online contact transaction, final cryptogram is a TC, and Issuer Authentication requirements are met
Contactless Transaction Counter Lower Limit (CLTCLL) F: b 8 T: 'DF21' in 'BF55' L: 1 S: Card	C If supported for contactless card velocity checking	Visa proprietary data element specifying the number of consecutive offline contactless domestic transactions allowed for that card application before a transaction is requested to go online.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (60 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Contactless Transaction Counter Upper Limit (CLTCUL) F: b 8 T: 'DF31' in 'BF55' L: 1 S: Card	C If supported for contactless card velocity checking	Visa proprietary data element specifying the maximum number of consecutive offline contactless domestic transactions allowed before the transaction is declined offline if it cannot be processed online	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.
Conversion Currency Code x F: n 3 T: Part of '9F73' L: 2 S: Card	C If currency conversion to be performed	Visa proprietary data element in the Currency Conversion Parameters data element that identifies an alternate currency to be converted (using Currency Conversion Factor x) to the designated currency in which the account is managed (Application Currency Code) according to ISO 4217.	UC: Modifiable IU: PUT DATA R: GET DATA (SD) (as part of '9F73')	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (61 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Counters Data Template F: b T: 'BF56' L: var S: Card	C If Profiles Functionality is supported and Consecutive Transaction card velocity checking is to be performed	Visa proprietary data template that contains the TLV-coded values for Consecutive Transaction Counters and their associated Limits and Upper Limits..	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the Counters Data Template: 'DF11': CTC 'DF21': CTCL 'DF31': CTCUL
Cryptogram Information Data (CID) F: b 8 T: '9F27' L: 1 S: Card	R	Indicates the type of cryptogram (TC, ARQC, or AAC) returned by the card and the actions to be performed by the terminal. The card shall never indicate to perform a referral.	UC: Transient IU: N R: GENERATE AC	bits 8–7 00b = AAC 01b = TC 10b = ARQC 11b = RFU bit 6–5: RFU (00b) bit 4: 1b = Advice required bits 3–1: (Reason/Advice Code): 000b = No information given 001b = Service not allowed 010b = PIN Try Limit exceeded 011b = Issuer Authentication failed xxxb = All other values are RFU Reset to all zeros during Initiate Application Processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (62 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cryptogram Version Number (CVN) F: b 8 T: Part of '9F10' L: 1 S: Card	R	Visa proprietary data element indicating the version of the TC/AAC/ARQC algorithm used by the application. Transmitted in the Issuer Application Data.	UC: Modifiable IU: PUT DATA to '9F10' R: GENERATE AC (part of Issuer Application Data, '9F10')	Values assigned by Visa. The left nibble of the byte indicates the format of Issuer Application Data. The only values supported in this version of VIS are: '0A' = CVN 10 '0C' = CVN 12 '12' = CVN 18 '22' = CVN '22' '2C' = CVN '2C' '32' - '3B' = CVN 50 through CVN 59

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (63 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cumulative Total Transaction Amount (CTTA) F: n 12 T: 'DF11' in 'BF58' L: 6 S: Card	C If Cumulative Total Transaction Amount card velocity checking is to be performed	Visa proprietary data element specifying the cumulative total amount of offline approved transactions in the designated currency (Application Currency Code) (or if currency conversion is supported, in a designated alternate currency) for the card application since the counter was reset.	UC: Dynamic IU: PUT DATA, CSU R: GENERATE AC (if included in the Issuer Discretionary Data Option supported as described in Appendix J) B: Backup or default to '9F54'	Initialized to zero unless optionally personalized to a starting value. Incremented by the Amount, Authorized each time a transaction in the designated currency is approved offline. Incremented by the Amount, Authorized approximated in the designated currency each time a transaction in a convertible currency is approved offline. Reset to zero: • if online transactions, final cryptogram is a TC, and Issuer Authentication requirements are met, and ADA allows reset during GENERATE AC. • if CTTAL is updated by an issuer script and ADA only allows reset with an issuer script.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (64 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cumulative Total Transaction Amount Funds (CTTA Funds) F: n 12 T: – L: 6 S: Card	O	Calculated value indicating the amount of offline funds available to spend in the Cumulative Total Transaction Amount.	UC: Transient IU: N R: N	Equal to the Cumulative Total Transaction Amount Upper Limit minus the Cumulative Total Transaction Amount. (CTTAUL - CTTA) If the Cumulative Total Transaction Amount Upper Limit is not present, equal to the Cumulative Total Transaction Amount Limit minus the Cumulative Total Transaction Amount.. (CTTAL - CTTA)
Cumulative Total Transaction Amount Limit (CTTAL) F: n 12 T: ' 'DF21' in 'BF58' L: 6 S: Card	C If Cumulative Total Transaction Amount Lower Limit card velocity checking is to be performed	Visa proprietary data element specifying the maximum total amount of offline approved transactions in the designated currency (Application Currency Code) (or if currency conversion is supported, in a designated alternate currency) allowed for the card application before a transaction is forced to go online.	UC: Modifiable IU: PUT DATA R: GET DATA (SD) GENERATE AC (if included in the Issuer Discretionary Data Option supported as described in Appendix J)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (65 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cumulative Total Transaction Amount Upper Limit (CTTAUL) F: n 12 T: 'DF31' in 'BF58' L: 6 S: Card	C If Cumulative Total Transaction Amount Upper Limit card velocity checking is to be performed	Visa proprietary data element specifying the maximum total amount of offline approved transactions in the designated currency (or (or if currency conversion is supported, in a designated alternate currency) allowed for the card application before a transaction is declined after an online transaction is unable to be performed.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. ***Note:*** *It is highly recommended that the Cumulative Total Transaction Amount Upper Limit be personalized if the Cumulative Total Transaction Amount Limit is personalized.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (66 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cumulative Total Transaction Amount x (CTTA x) F: n 12 T: 'DF1x' in 'BF58' L: 6 S: Card	C If Profiles Functionality is supported and Cumulative Total Transaction Amount card velocity checking is to be performed	If multiple CTTAs are supported for Profiles, then the 'x' in the tag identifies which CTTA x is identified by the tag (e.g. CTTA 1 is 'DF11' in 'BF58', CTTAUL 4 is 'DF14' in 'BF58').	UC: Dynamic IU: PUT DATA, CSU R: GET DATA (SD) B: Backup or default to 'DF3x' in 'BF58'	Initialized to zero unless optionally personalized to a starting value. If counting is allowed for the Profile: • incremented by the Amount, Authorized each time a transaction in the designated currency is approved offline • incremented by the Amount, Authorized approximated in the designated currency each time a transaction in a convertible currency is approved offline. If reset is allowed for the Profile, reset to zero: • if online transactions, final cryptogram is a TC, and Issuer Authentication requirements are met, and ADA allows reset during GENERATE AC. • if CTTAL x is updated by an issuer script and ADA only allows reset with an issuer script.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (67 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cumulative Total Transaction Amount x Funds (CTTA x Funds) F: n 12 T: – L: 6 S: Card	O	If multiple CTTA Funds are supported for Profiles, then the 'x' identifies which CTTA x Funds is identified.	UC: Transient IU: N R: N	
Cumulative Total Transaction Amount Limit x (CTTAL x) F: n 12 T: 'DF2x' in 'BF58' L: 6 S: Card	C If Profiles Functionality is supported and Cumulative Total Transaction Amount Lower Limit card velocity checking is to be performed	If multiple CTTALs are supported for Profiles, then the 'x' in the tag identifies which CTTAL x is identified by the tag (e.g. CTTAL 1 is 'DF21' in 'BF58', CTTAL 4 is 'DF24' in 'BF58').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (68 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Cumulative Total Transaction Amount Upper Limit x (CTTAUL x) F: n 12 T: 'DF3x' in 'BF58' L: 6 S: Card	C If Profiles Functionality is supported and Cumulative Total Transaction Amount Upper Limit card velocity checking is to be performed	If multiple CTTAULs are supported for Profiles, then the 'x' in the tag identifies which CTTAUL x is identified by the tag (e.g. CTTAUL 1 is 'DF31' in 'BF58', CTTAUL 4 is 'DF34' in 'BF58').	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization. ***Note:*** *It is highly recommended that the Cumulative Total Transaction Amount Upper Limit x be personalized if the associated Cumulative Total Transaction Amount Limit x is personalized.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (69 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Currency Conversion Factor x F: n 8 T: Part of '9F73' L: 4 S: Card	C If currency conversion to be performed	Visa proprietary data element in the Currency Conversion Parameters data element that specifyies a decimal value used in a conversion algorithm to convert an amount in the currencyidentified by Conversion Currency Code x to the designated currency in which the account is managed (Application Currency Code). This rate is an approximation and should be limited to two significant digits.	UC: Modifiable IU: PUT DATA R: GET DATA (SD) (as part of '9F73')	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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (70 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Currency Conversion Parameters F: n T: '9F73' L: var. S: Card	C If currency conversion is to be performed in the card	A Visa proprietary data element specifying the currency code and conversion factor for converting an amount in an alternate currency to an approximate value in the designated currency in which the account is managed. Conversion Parameters contains one or more sets consisting of a Conversion Currency Code and an associated Currency Conversion Factor. Applications that support Currency Conversion shall be able to support up to five alternate currencies.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Bytes: 1–2: Conversion Currency Code 1 3–6: Currency Conversion Factor 1 7–8: Conversion Currency Code 2 9–12: Currency Conversion Factor 2 13–14: Conversion Currency Code 3 15–18: Currency Conversion Factor 3 19–20: Conversion Currency Code 4 21–24: Currency Conversion Factor 4 25–26: Conversion Currency Code 5 27–30: Currency Conversion Factor 5
Data Authentication Code F: b 16 T: '9F45' L: 2 S: Card	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 ('93').	UC: Modifiable (as part of '93') IU: UPDATE RECORD (to record containing '93') R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (71 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Dedicated File (DF) Name F: b 40–128 T: '84' L: 5–16 S: Card	R	Identifies the name of the DF as described in ISO/IEC 7816-4.	UC: Unchanging IU: N R: SELECT	
Default Dynamic Data Authentication Data Object List (Default DDOL) F: b T: – L: var. S: Terminal	C If DDA or CDA is supported	DDOL to be used for constructing the INTERNAL AUTHENTICATE command if the DDOL in the card is not present.	n/a	Shall contain the tag for Unpredictable Number ('9F37') only.
Default Transaction Certificate Data Object List (Default TDOL) F: b T: – L: var. S: Terminal	O	TDOL to be used to generate the TC Hash Value if the TDOL in the card is not present. Not currently used in any VIS cryptograms defined by Visa.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (72 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Derivation Key Index (DKI) F: b 8 T: Part of '9F10' L: 1 S: Card	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.	UC: Modifiable IU: PUT DATA to '9F10' R: GENERATE AC (part of Issuer Application Data, '9F10')	Value assigned by the issuer. If only one key or key pair is used by the issuer, then a value of zero may be used.
Directory Definition File (DDF) Name F: b 40–128 T: '9D' L: 5–16 S: Card	C If directory selection is supported	Identifies the name of the DF associated with a directory.	UC: Unchanging IU: N R: SELECT	
Directory Discretionary Template F: var. T: '73' L: var. up to 252 S: Card	O	Issuer discretionary part of the directory according to ISO/IEC 7816-5.	UC: Unchanging IU: N R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (73 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Dynamic Data Authentication Data Object List (DDOL) F: b T: '9F49' L: var. up to 252 S: Card	C If DDA is supported	List of data objects (tags and lengths) to be passed to the ICC in the INTERNAL AUTHENTICATE command.	UC: Unchanging IU: N R: READ RECORD	
Dynamic Data Authentication Failure Indicator F: b 1 T: – L: – S: Card	C If DDA or CDA is supported	Visa proprietary data element that indicates whether offline dynamic data authentication failed on the last transaction when that transaction was declined offline.	UC: Persistent IU: N R: N B: Backup or default to 0b	bit 1: 1b = Offline dynamic data authentication failed on last transaction and transaction declined offline Set to 1b during Offline Data Authentication if DDA or CDA fails and the transaction is declined offline. Reset to 0b if online transaction (either approved or declined) and Issuer Authentication requirements are me.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (74 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Enciphered Personal Identification Number (PIN) Data F: b 64 T: – L: 8 S: Terminal	C If online PIN supported or if PIN pad and card reader separate	Transaction PIN enciphered at the PIN pad for online verification or for offline verification if the PIN pad and the interface device (IFD) are not a single integrated device.	n/a	
Entry Length F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Indicates the length of the Profile Selection Entry (not including Entry Length) .	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	
File Control Information (FCI) Issuer Discretionary Data F: var. T: 'BF0C' L: var. up to 222 S: Card	C If transaction logging is supported	Issuer discretionary part of the FCI.	UC: Unchanging IU: N R: SELECT	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (75 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
File Control Information (FCI) Proprietary Template F: var. T: 'A5' L: var. S: Card	R	Identifies the data objects proprietary to EMV in the FCI Template according to ISO/IEC 7816-4.	UC: Unchanging IU: N R: SELECT	
File Control Information (FCI) Template F: var. T: '6F' L: var. up to 252 S: Card	R	Identifies the FCI template according to ISO/IEC 7816-4.	UC: Unchanging IU: N R: SELECT	
Go Online On Next Transaction Indicator F: b 1 T: – L: – S: Card	C If CVN 18 supported	Visa proprietary data element indicating that in the online response of a previous transaction, the issuer indicated that subsequent transactions should go online.	UC: Modifiable IU: CSU R: N	Set to 1b during Completion if the 'Set go online on next transaction' bit of the last verified CSU was set to 1b. Reset to 0b of a subsequent online transaction if Issuer Authentication requirements are met

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (76 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Integrated Circuit Card (ICC) Dynamic Data F: – T: – L: var. S: Card	C If DDA or CDA supported	Issuer-determined dynamic data generated by 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.	UC: Transient IU: N R: INTERNAL AUTHENTICATE	The ICC Dynamic Number is the first data element in the ICC Dynamic Data.
Integrated Circuit Card (ICC) Dynamic Number F: b T: '9F4C' L: 2–8 S: Card	C If DDA or CDA supported	Time-variant number generated by the card during DDA or CDA and included in the Signed Dynamic Application Data (tag '9F4B') passed to the terminal. Recovered by the terminal.	UC: Transient IU: N R: INTERNAL AUTHENTICATE	The Application Transaction Counter (ATC) is the first data element of the ICC Dynamic Number. The ATC in ICC Dynamic Number may be either in plaintext or encrypted.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (77 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Integrated Circuit Card (ICC) PIN Encipherment Private Key F: b T: – L: N_{PE} S: Card	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.	UC: Unchanging IU: N R: N Secret	If supported, applications shall at least support ICC PIN Encipherment Private Key lengths up to and including 1408 bits. Applications may support longer keys. Issuers may personalize shorter keys. ***Note:*** *Issuers should check with their regional representative before using an ICC PIN Encipherment Private Key of 1024 bits or longer.*
Integrated Circuit Card (ICC) PIN Encipherment Public Key Certificate F: b T: '9F2D' L: N_{PE} S: Card	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.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (78 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Integrated Circuit Card (ICC) PIN Encipherment Public Key Exponent F: b T: '9F2E' L: 1 or 3 S: Card	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.	UC: Unchanging IU: N R: READ RECORD	3 or (2^{16} + 1). ***Note:*** *Visa recommends using the value 3.*
Integrated Circuit Card (ICC) PIN Encipherment Public Key Remainder F: b T: '9F2F' L: N_{PE} - N_I + 42 S: Card	C If the entire public key does not fit in the corresponding certificate	Digits of the ICC PIN Encipherment Public Key Modulus that do not fit into the ICC PIN Encipherment Public Key Certificate.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (79 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Integrated Circuit Card (ICC) Private Key F: b T: – L: N_{IC} S: Card	C If DDA or CDA is supported Or 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.	UC: Unchanging IU: N R: N Secret	If supported, applications shall support ICC Private Key lengths up to and including 1408 bits. Applications may support longer keys. Issuers may personalize shorter keys. ***Note:*** *Issuers should check with their regional representative before using an ICC Private Key of 1024 bits or longer.*
Integrated Circuit Card (ICC) Public Key Certificate F: b T: '9F46' L: N_I S: Card	C If DDA or CDA is supported. Or 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.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (80 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Integrated Circuit Card (ICC) Public Key Exponent F: b T: '9F47' L: 1 or 3 S: Card	C If DDA or CDA is supported Or 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.	UC: Unchanging IU: N R: READ RECORD	3 or (2^{16} + 1). ***Note:*** *Visa recommends using the value 3.*
Integrated Circuit Card (ICC) Public Key Remainder F: b T: '9F48' L: N_{IC} - N_I + 42 S: Card	C If the entire public key does not fit in the corresponding certificate	Digits of the ICC Public Key Modulus which do not fit within the ICC Public Key Certificate.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	
Interface Device (IFD) Serial Number F: an 8 T: '9F1E' L: 8 S: Terminal	R	Unique and permanent serial number assigned to the IFD by the manufacturer.	n/a	Value assigned by IFD manufacturer.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (81 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
International Bank Account Number (IBAN) F: var. T: '5F53' L: up to 34 S: Card	O	Uniquely identifies the account of a customer at a financial institution as defined in ISO 13616. In template 'BF0C' or '73'.	UC: Unchanging IU: N R: READ RECORD, SELECT	
International Counters Data Template F: b T: 'BF57' L: var S: Card	C If Profiles Functionality is supported and Consecutive International Transactions or Consecutive International Country Transactions card velocity checking is to be performed	Visa proprietary data template that contains the TLV-coded values for Consecutive Transaction Counters and their associated Limits and Upper Limits..	UC: Dynamic IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the Counters Data Template: 'DF11': CTCI 'DF21': CTCIL 'DF31': CTIUL 'DF51': CTCIC 'DF61': CTCICL

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (82 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Action Code—Default F: b 40 T: '9F0D' L: 5 S: Card	R	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.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Bit assignments are identical to those for Terminal Verification Results (TVR).
Issuer Action Code—Denial F: b 40 T: '9F0E' L: 5 S: Card	R	Specifies the issuer's conditions that cause the decline of a transaction without attempting to go online.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Bit assignments are identical to those for Terminal Verification Results (TVR).
Issuer Action Code—Online F: b 40 T: '9F0F' L: 5 S: Card	R	Specifies the issuer's conditions that cause a transaction to be transmitted online.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Bit assignments are identical to those for Terminal Verification Results (TVR).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (83 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Application Data (IAD) F: b T: '9F10' L: var. up to 32 S: Card	R	Contains proprietary application data for transmission to the issuer. This version of VIS supports the following IAD formats: • IAD Format 0/1/3 • IAD Format 2, as defined in section F, Issuer Application Data and Card Verification Results Formats. If the IAD complies with IAD Format 0/1/3, then: • Byte 1: length of the Visa Discretionary Data ('06') • Byte 2: Derivation Key Index (DKI) • Byte 3: Cryptogram Version Number (CVN) • Byte 4–7: Card Verification Results (CVR), including the 1-byte length indicator. - continues -	UC: See the capability for individual IAD components IU: PUT DATA (only the DKI, CVN, and Issuer Discretionary Data may be modified) R: GENERATE AC	If the Issuer Discretionary Data is personalized with the Issuer Discretionary Data Identifier (IDD ID) and IDD Length as described in Appendix J, the application includes the values of internal application data elements in the Issuer Discretionary Data portion of the Issuer Application Data (see Issuer Discretionary Data Option Identifier for defined values).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (84 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Application Data (IAD) (continued)		IAD Format 0/1/3, continued: • If Issuer Discretionary Data is present – Byte 8: Length of Issuer Discretionary Data – Bytes 9–23: concatenated issuer discretionary data If the IAD complies with IAD Format 2, then: • Byte 1: length of the IAD ('1F') • Byte 2: CVN (the left nibble indicates the IAD Format) • Byte 3: DKI • Byte 4–8: CVR • Byte 9–32: concatenated issuer discretionary data		

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (85 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Authentication Data (IAuD) F: b 64–128 T: '91' L: 8–16 S: Issuer	O Passed from issuer through terminal if Issuer Authentication is supported	Issuer data transmitted to card for Issuer Authentication. The Issuer Authentication Data consists of the following for CVN 10, CVN 12, or CVN 50 through CVN 59: • ARPC – first 8 bytes • ARPC Response Code – 2 bytes immediately following ARPC The Issuer Authentication Data consists of the following for CVN 18: • ARPC – first 4 bytes • CSU – 4 bytes immediately following ARPC • optional Proprietary Authentication Data – 1-8 bytes immediately following CSU	n/a	***Note:*** *The optional Proprietary Authentication Data for CVN 18 or CVN '22' is only supported for Field 55 issuers. The use of Proprietary Authentication Data is beyond the scope of this specification.* ***Note:*** *Third bit map issuers may send the 2-byte ARPC Response Code as part of Issuer Authentication Data sent in the online response for CVN 18 or CVN '22', but the 'Proprietary Authentication Data included' bit of the CSU shall be set to 0b, and the ARPC Response Code is not processed as optional Proprietary Authentication Data when generating the ARPC for CVN 18.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (86 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Authentication Failure Indicator F: b 1 T: – L: – S: Card	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	UC: Persistent IU: N R: N B: Backup or default to 0b or 1b	bit 1: 1b = Issuer Authentication failure on last online transaction Set to 1b: • during Issuer Authentication processing if Issuer Authentication fails. • during Completion If Issuer Authentication is mandatory and not performed. Reset to 0b when Issuer Authentication passes on a subsequent transaction

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (87 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Authentication Indicator F: b 8 T: '9F56' L: 1 S: Card	C If Issuer Authentication is supported	Visa proprietary data element indicating when Issuer Authentication is supported, whether it is mandatory or optional. When this data element is present (either personalized on the card, or added to the card post-issuance using a PUT DATA issuer script command), the application supports Issuer Authentication Data.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	***Note:*** *Visa recommends this data element be personalized (to indicate that Issuer Authentication is supported).* ***Note:*** *This data element shall be personalized for cards that also support offline-capable contactless functionality in qVSDC.* bit 8: 1b = Issuer Authentication mandatory 0b = Issuer Authentication optional bits 7–1: RFU (0000000b) ***Note:*** *Issuer Authentication Indicator bit 8 shall be set to 1b for cards that also support offline-capable contactless functionality such as qVSDC.* ***Note:*** *Visa highly recommends that Issuer Authentication be mandatory, except for early acquiring markets.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (88 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Authentication Performed Using EXTERNAL AUTHENTICATE **Command Indicator** F: b 1 T: – L: – S: Card	C If Issuer Authentication is supported for CVN 10	Visa proprietary data element indicating that Issuer Authentication was performed during the current transaction using the EXTERNAL AUTHENTICATE command.	UC: Transient IU: N R: N	Set to 1b during EXTERNAL AUTHENTICATE command processing. Reset at the beginning of each transaction.
Issuer Code Table Index F: n 2 T: '9F11' L: 1 S: Card	C If Application Preferred Name is present	Indicates the code table according to ISO/IEC 8859 for displaying the Application Preferred Name.	UC: Unchanging IU: N R: SELECT	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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (89 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Country Code F: n 3 T: '5F28' L: 2 S: Card	C If Application Usage Control is present	Indicates the country of the issuer, represented according to ISO 3166.	UC: Unchanging IU: N R: READ RECORD	Shall match the value of '9F57'.
Issuer Country Code F: n 3 T: '9F57' L: 2 S: Card	C If Consecutive International Country Transactions card velocity checking is to be performed or Consecutive International Transactions card velocity checking includes international country transactions and is to be performed	Visa proprietary data element indicating the country of the issuer, represented according to ISO 3166.	UC: Unchanging IU: N R: GET DATA (SD)	Shall match the value of '5F28'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (90 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Country Code (alpha2) F: a2 T: '5F55' L: 2 S: Card	O	Indicates the country of the issuer as defined in ISO 3166 (using a 2 character alphabetic code). In template 'BF0C' or '73'.	UC: Unchanging IU: N R: READ RECORD, SELECT	
Issuer Country Code (alpha3) F: a2 T: '5F56' L: 2 S: Card	O	Indicates the country of the issuer as defined in ISO 3166 (using a 3 character alphabetic code). In template 'BF0C' or '73'.	UC: Unchanging IU: N R: READ RECORD, SELECT	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (91 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Discretionary Data Identifier (IDD ID) F: b 8 T: Part of '9F10' L: 1 S: Card	O	Visa proprietary data element indicating the format of issuer discretionary data transmitted in the Issuer Application Data. Optionally transmitted to the issuer in the Issuer Application Data. IDD option '0' (issuer-defined) is the only value supported for IAD Format '2'.	UC: Modifiable IU: PUT DATA to '9F10' R: GENERATE AC (part of Issuer Application Data, '9F10')	bits 8–5: RFU (0000b) bits 4–1: IDD Option ID (IDDO ID): Identifies the contents in the remaining bytes of issuer discretionary data: '0' = Issuer-defined ***Note:*** *If the Issuer Discretionary Data requires a MAC (such as for CVN 10), then a MAC on the Issuer Discretionary Data is calculated as described in Appendix J and is appended to the IDD contents for IDDO IDs other than '0'.* '1' = VLP Available Funds ***Note:*** *A value of '1' will not be supported in future versions of the specification. Issuers should instead use IDDO ID '3'.* *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (92 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Discretionary Data Identifier (IDD ID) (continued)				bits 4–1, continued: '2' = Cumulative Total Transaction Amount ***Note:*** *A value of '2' will not be supported in future versions of the specification. Issuers should instead use IDDO ID '4'.* '3' = VLP Available Funds followed by Cumulative Total Transaction Amount '4' = Cumulative Total Transaction Amount followed by Cumulative Total Transaction Amount Limit '5' = Available Offline Spending Amount '6' = Available Offline Spending Amount followed by Last Successful Issuer Update ATC Register followed by Issuer Script Command Counter '7' – 'F' = RFU

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (93 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Identification Number (IIN) F: n6 T: '42' L:3 S: Card	O	Number that identifies the major industry and the card issuer and that forms part of the Primary Account Number (PAN). In template 'BF0C' or '73'.	UC: Unchanging IU: N R: READ RECORD, SELECT	
Issuer Public Key Certificate F: b T: '90' L: N_{CA} S: Card	C If SDA, DDA, CDA, or Offline Enciphered PIN supported	Issuer's public key certified by a certificate authority for use in offline static and dynamic data authentication.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	
Issuer Public Key Exponent F: b T: '9F32' L: 1 or 3 S: Card	C If SDA, DDA, CDA, or Offline Enciphered PIN supported	Issuer public key exponent used for the verification of the Signed Static Application Data and the ICC Public Key Certificate.	UC: Unchanging IU: N R: READ RECORD	3 or (2^{16} + 1). ***Note:*** *Visa recommends using the value 3.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (94 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Public Key Remainder F: b T: '92' L: $N_I - N_{CA} + 36$ S: Card	C If the entire public key does not fit in the corresponding certificate	Portion of the Issuer Public Key Modulus which does not fit into the Issuer PK Certificate.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	
Issuer Script Command F: b T: '86' L: var. up to 261 S: Issuer	O From issuer to terminal. Passed to card	Sent in authorization response from issuer when response contains Issuer Script. Contains command passed to card.	n/a	See Appendix C, Commands for Financial Transactions. ***Note:*** *EMV specifies that terminals and networks must support a total length for all issuer scripts in an online response of up to 128 bytes. Issuers may send longer issuer scripts only when the issuer knows that longer issuer scripts are supported by all entities transporting the script back to the card.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (95 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Script Command Counter F: b 4 T: – L: – S: Card	C If Issuer Script is supported	Visa proprietary data element that indicates the number of Issuer Script Commands processed by the card. Script commands are counted regardless of whether they are received before or after the second GENERATE AC.	UC: Persistent IU: N R: GENERATE AC B: Backup	bits 4–1: Number of Issuer Script Commands Incremented by 1 during Issuer Script processing for each script command received with secure messaging . If thecounter is **not** cyclic: • Count Issuer Script commands received that contain secure messaging • Reset to '0' if online transaction (either approved or declined) and Issuer Authentication requirements are met. • A value of 'F' is equivalent to 15 or more Issuer Script Commands. If the counter **is** cyclic: • Count issuer script commands that were successfullly completed. • The counter shall never be reset. • When the counter reaches the maximum value ('F'), it rolls over from 'F' to '0' and continues incrementing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (96 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Script Failure Indicator F: b 1 T: – L: – S: Card	C If Issuer Script is supported	Visa proprietary data element that indicates whether Issuer Script processing failed.	UC: Persistent IU: N R: N B: Backup or default to 0b or 1b	bit 1: 1b = Issuer Script processing failed Set to 1b 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 0b if online transaction (either approved or declined) and Issuer Authentication requirements are met
Issuer Script Identifier F: b 32 T: '9F18' L: 4 S: Issuer	O From issuer to terminal. Not passed to card.	May be sent in authorization response from issuer when response contains Issuer Script. Assigned by the issuer to uniquely identify the Issuer Script.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (97 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Script Results F: b T: '9F5B' L: var. S: Terminal	R	Indicates the results of Issuer Script processing. ***Note:*** *When the terminal transmits this data element to the acquirer, in this version of VIS, it is acceptable that only byte 1 is transmitted, although it is preferable for all 5 bytes to be transmitted.*	n/a	Byte 1(Issuer Script Result): bits 8-5: Result of the Issuer Script processing performed by the terminal: '0' = Issuer Script not performed '1' = Issuer Script processing failed '2' = Issuer Script processing successful bits 4-1: Sequence number of the Issuer Script Command: '0' = Not specified '1'-'E' = Sequence number 1-14 'F' = Sequence number 15 or above Bytes 2-5 (Issuer Script Identifier): Issuer Script Identifier received by the terminal, if available; zero filled if not available. Mandatory if more than one Issuer Script was received by the terminal.

- continues -

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (98 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer Script Results (continued)				Bytes 1-5 are repeated for each Issuer Script processed by the terminal, although in this version of VIS, only one Issuer Script may be transmitted in the response message.
Issuer Script Template 1 F: b T: '71' L: var. S: Issuer	O	Contains proprietary issuer data for transmission to the card before the second GENERATE AC command. Use of this data object is not recommended in this version of VIS.	n/a	***Note:*** *EMV specifies that terminals and networks must support a total length for all issuer scripts in an online response of up to 128 bytes. Issuers may send longer issuer scripts only when the issuer knows that longer issuer scripts are supported by all entities transporting the script back to the card.*
Issuer Script Template 2 F: b T: '72' L: var. S: Issuer	C If Issuer Script is supported	Contains proprietary issuer data for transmission to the card after the final GENERATE AC command.	n/a	***Note:*** *EMV specifies that terminals and networks must support a total length for all issuer scripts in an online response of up to 128 bytes. Issuers may send longer issuer scripts only when the issuer knows that longer issuer scripts are supported by all entities transporting the script back to the card.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (99 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Issuer URL F: ans T: '5F50' L: var. S: Card	not applicable	The URL provides the location of the issuer's Library Server on the Internet. Not used in this version of VIS.	n/a	
Language Preference F: an 2 T: '5F2D' L: 2–8 S: Card	O	1–4 languages stored in order of preference, each represented by 2 lower case alphabetical characters according to ISO/FDIS 639.	UC: Unchanging IU: N R: SELECT	
Last Contactless Application Cryptogram Valid Indicator F: – T: – L: – S: Card	C If Issuer Update processing is supported for contactless	Proprietary Visa data element indicating whether the Last Contactless Application Cryptogram is valid for contactless Issuer Update processing.	UC: Persistent IU: N R: N	bit 1: 1b = Last Contactless Application Cryptogram valid Initial value is zero. Reset to 0b during Initiate Application Processing for contact transactions. Set by contactless transactions. See the *Visa Contactless Payment Specification* for further explanation of the Last Contactless Application Cryptogram Valid Indicator and contactless Issuer Update processing.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (100 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Last Online Application Transaction Counter (ATC) Register F: b 16 T: '9F13' L: 2 S: Card	C If terminal velocity check (LCOL or UCOL) or card or terminal new card check is to be performed	ATC value of the last transaction that went online.	UC: Persistent IU: N R: GET DATA (if terminal velocity checking or new card check is to be performed) B: Backup or default to '0001'	Initial value is zero. Reset to current value of ATC if online transaction, final cryptogram is a TC, and Issuer Authentication requirements are met
Last Successful Issuer Update ATC Register F: b 16 T: – L: 2 S: Card	C If Issuer Update processing is supported for contactless	Proprietary Visa data element containing the ATC value from the last successful Issuer Update (either as a result of Issuer Authentication or Issuer Scripting). See the *Visa Contactless Payment Specification*. ***Note:*** *This data element is not supported for contact-only implementations.*	UC: Persistent IU: N R: First GENERATE AC (if included in the IDD as specified in Appendix E of the *Visa Contactless Payment Specification (VCPS);* see the VCPS for Retrieval Requirements over the contactless interface).	Initial value is zero. Reset to current value of ATC if online transaction and either Issuer Authentication requirements are met or an issuer script command is successfully processed.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (101 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values	
Log Entry F: b T: '9F4D' L: 2 S: Card	C If transaction logging is to be supported	Devices that read the transaction log use the Log Entry data element to determine the location (SFI) and the maximum number of transaction log records.	UC: Unchanging IU: N R: SELECT	Byte 1 Byte 2	SFI containing the cyclic transaction log file. Maximum number of records in the transaction log file.
Log Format F: b T: '9F4F' L: var. S: Card	C If transaction logging is to be supported	List in tag and length format of data elements that are logged by the transaction.	UC: Unchanging IU: N R: GET DATA (SD)		

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (102 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Lower Consecutive Offline Limit (LCOL) F: b 8 T: '9F14' L: 1 S: Card	C If terminal velocity check (LCOL or UCOL) or terminal new card check is to be performed	Issuer-specified preference for maximum number of consecutive offline transactions allowed for the application in a terminal with online capability.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD B: Backup	
Maximum Target Percentage to be Used for Biased Random Selection F: – T: – L: – S: Terminal	C If offline capable terminal	Value used in terminal risk management for random transaction selection.	n/a	
Merchant Category Code F: n 4 T: '9F15' L: 2 S: Terminal	R	Classifies the type of business being done by the merchant, represented according to ISO 8583:1993 for Card Acceptor Business Code.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (103 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Merchant Identifier F: ans 15 T: '9F16' L: 15 S: Terminal	R (at terminal or acquirer)	When concatenated with the Acquirer Identifier, uniquely identifies a given merchant within a given country. May be located in the terminal or inserted into messages by the acquirer.	n/a	
Merchant Name and Location F: ans T: '9F4E' L: var. S: Terminal	R (at terminal or acquirer)	Indicates the name and location of the merchant. May be located in the terminal or inserted into messages by the acquirer.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (104 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Negative Action F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Indicates the action to be taken by the application if the Check Type test result is **false**. The Negative Action byte indicates one of the following: • Profile ID to use for the Transaction • Number of Profile Selection Entries to Skip	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	bit 8. 1b = Bits 7-1 of Negative Action indicate the number of Profile Selection Entries in the Profile Selection File to skip down before continuing processing the next Profile Selection Entry. 0b = Negative Action byte contains the Profile ID to use for the transaction. bits 7-1 Contain either: – the number of Profile Selection Entries to skip down (if bit 8 = 1b) – remainder of the Profile ID to use (if bit 8 = 0b) If the value is: '7F' = Discontinue processing the GPO command and respond with SW1 SW2 = '6985'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (105 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Number of Blocks F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Indicates the number of Comparison Blocks in the Profile Selection Entry. The first Comparison Block is a Bit Mask. The second and any subsequent Comparison Blocks are Comparison Value(s) that are compared to the data extracted from the Profile Selection Input Data.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (106 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Offline Decline Requested by Card Indicator F: b 1 T: – L: – S: Card	C If card risk management check can generate a decline	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.	UC: Transient IU: N R: N	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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (107 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Online Authorization Indicator F: b 1 T: – L: – S: Card	C If Issuer Authentication or Issuer Script is supported	Visa proprietary data element indicating whether the card requested an ARQC and the transaction was not completed.	UC: Persistent IU: N R: N B: Backup or default to 1b	bit 1: 1b = Online authorization required and online not completed on current or previous transaction Set to 1b during Card Action Analysis if ARQC is requested by the card. Reset to 0b if online authorization (either approval or decline) and Issuer Authentication requirements are met.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (108 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Online Requested by Card Indicator F: b 1 T: – L: – S: Card	C If offline PIN verification or card risk management check can generate an online request	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.	UC: Transient IU: N R: N	Set during Card Action Analysis: • If Online Authorization Indicator = 1b • 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 Reset at the beginning of each transaction.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (109 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Payment Account Reference (PAR) T: '9F24' S: Card * See [EMV Tokenisation] for format and length information.	O This data element may be present on cards that have been tokenized	Uniquely identifies the underlying cardholder account to which a payment token is associated, as defined in [EMV Tokenisation].	UC: Unchanging IU: N R: READ RECORD	See [EMV Tokenisation].
Personal Identification Number (PIN) Pad Secret Key F: – T: – L: – S: Terminal	C If PIN pad and card reader not integrated	Secret key of a symmetric algorithm used by the PIN pad to encipher the PIN and by the card reader to decipher the PIN if the PIN pad and card reader are not integrated. ***Note:*** *This is* not *the key used for Offline Enciphered PIN.*	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (110 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Personal Identification Number (PIN) Try Counter F: b 8 T: '9F17' L: 1 S: Card	C If offline PIN is supported	Number of PIN tries remaining.	UC: Dynamic IU: PIN CHANGE/ UNBLOCK or CSU R: GET DATA (If "Last PIN Attempt" is to display) B: Backup or default to PIN Try Limit	Initial value is personalized to an issuer-defined value. Decremented by 1 each time an incorrect PIN is entered or there is an error deciphering an offline enciphered PIN. Reset to the PIN Try Limit when the correct PIN is entered or when the PIN is changed or unblocked by the issuer. May be updated to a value less than or equal to the PIN Try Limit using the CSU for CVN 18 if Issuer Authentication passes. The value shall be less than or equal to 15 ('0F').
Personal Identification Number (PIN) Try Limit F: b 8 T: – L: 1 S: Card	C If offline PIN is supported	Visa proprietary data element containing the issuer-specified maximum number of consecutive incorrect PIN tries allowed.	UC: Modifiable IU: n/a R: N	Initial value is personalized to an issuer-defined value. ***Note:*** *Example methods for personalizing the initial value include setting the PIN Try Limit to the value personalized in the PIN Try Counter, or personalizing the initial value in a fixed-format DGI using EMV-CPS.* The value shall be less than or equal to 15 ('0F').

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (111 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Position in Profile Selection Input Data (Position) F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Indicates the starting position (in bytes) of the portion of Profile Selection Input Data that is used as extracted data input for processing a single Profile Selection Entry in the Profile Selection process.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	If the first byte of Profile Selection Input Data is to be used as the first byte in the extracted data, then the value of Position is '01'. For Check Types that do not use Profile Selection Input Data (for example, Check Types '2x', '3x', '4x', or '52'), Position should be '00'.
Positive Action F: b 8 T: – L: 1 S: Card	C If Profiles Functionality is supported	Part of a Profile Selection Entry in the Profile Selection File. Indicates the action to be taken by the application if the Check Type test result is **true**. The Positive Action byte indicates one of the following: • Profile ID to use for the Transaction • Number of Profile Selection Entries to Skip	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	bit 8. 1b = Bits 7-1 of Positive Action indicate the number of Profile Selection Entries in the Profile Selection File to skip down before continuing processing the next Profile Selection Entry. 0b = Positive Action byte contains the Profile ID to use for the transaction. bits 7-1 Contain either: – the number of Profile Selection Entries to skip down (if bit 8 = 1b) – remainder of the Profile ID to use (if bit 8 = 0b) If the value is: '7F' = Discontinue processing the GPO command and respond with SW1 SW2 = '6985'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (112 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Processing Options Data Object List (PDOL) F: b T: '9F38' L: var. S: Card	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.	UC: Unchanging IU: N R: SELECT	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (113 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Control x F: b T: 'DF1x' in 'BF59' L: var. 10 to32 S: Card	C If Profiles Functionality is supported	Configures the application data and behavior to be used for transactions conducted using the profile.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Byte 1 (AIP and AFL): bits 8–5: AIP/AFL Entry ID - Indicate which AIP and AFL Entry to use for the Profile x '1' = Use AIP/AFL Entry 1 '2' = Use AIP/AFL Entry 2 '3' = Use AIP/AFL Entry 3 '4' = Use AIP/AFL Entry 4 bits 4–1: RFU ('0') Byte 2 (Profile-specific ADA Options): bit 8: 1b = If Issuer Authentication failure, transmit next transaction online bit 7: 1b = If new card, transmit transaction online bit 6: 1b = If new card, decline if unable to transmit transaction online bit 5: 1b = If PIN Try Limit exceeded on previous transaction, transmit transaction online bit 4: 1b = If Issuer Script failed on a previous transaction, transmit transaction online bit 3: 1b = Log transaction performed using this profile bits 2-1: RFU (00b) *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (114 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Control x (continued)		***Note:*** *The "Check limits" bit for a counter cause the application to check a counter against its limits without allowing counting in the profile.* ***Note:*** *The "Allow counting" bit for a counter cause the application to check a counter against its limits and allows counting in the profile.* ***Note:*** *The "Allow reset" bit for a counter allows the counter to be reset to zero or the upper limit in the profile.*		Byte 3 (CTTA 1 & CTTA 2 controls): ***Note:*** *CTTA = Cumulative Total Transaction Amount* bit 8: 1b = Check limits for CTTA 1 bit 7: 1b = Allow counting in CTTA 1 bit 6: 1b = Allow reset of CTTA 1 bit 5: 1b = Check limits for CTTA 2 bit 4: 1b = Allow counting in CTTA 2 bit 3: 1b = Allow reset of CTTA 2 bits 2-1: RFU (00b) ***Note:*** *If the 'Do not reset CTTA during GENERATE AC' bit af the ADA has the value 1b, bits 6 & 3 should be set to 0b for all profiles.* Byte 4 (CTC 1 & CTC 2 controls): ***Note:*** *CTC = Consecutive Transaction Counter* bit 8: 1b = Check limits for CTC 1 bit 7: 1b = Allow counting in CTC 1 bit 6: 1b = Allow reset for CTC 1 bit 5: 1b = Check limits for CTC 2 bit 4: 1b = Allow counting in CTC 2 bit 3: 1b = Allow reset for CTC 2 bits 2-1: RFU (00b) *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (115 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Control x (continued)				Byte 5 (CTCI 1 & CTCI 2 controls): ***Note:*** *CTCI = Consecutive Transaction Counter International* bit 8: 1b = Check limits for CTCI 1 bit 7: 1b = Allow counting in CTCI 1 bit 6: 1b = Allow reset for CTCI 1 bit 5: 1b = Check limits for CTCI 2 bit 4: 1b = Allow counting in CTCI 2 bit 3: 1b = Allow reset for CTCI 2 bits 2-1: RFU (00b) Byte 6 (CTCIC 1 & CTCIC 2 controls): ***Note:*** *CTCIC = Consecutive Transaction Counter International Country* bit 8: 1b = Check limits for CTCIC 1 bit 7: 1b = Allow counting in CTCIC 1 bit 6: 1b = Allow reset for CTCIC 1 bit 5: 1b = Check limits for CTCIC 2 bit 4: 1b = Allow counting in CTCIC 2 bit 3: 1b = Allow reset for CTCIC 2 bits 2-1: RFU (00b) *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (116 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Control x (continued)				Byte 7 (CTTA 3 & CTTA 4 controls): ***Note:*** *CTTA = Cumulative Total Transaction Amount* bit 8: 1b = Check limits for CTTA 3 bit 7: 1b = Allow counting in CTTA 3 bit 6: 1b = Allow reset of CTTA 3 bit 5: 1b = Check limits for CTTA 4 bit 4: 1b = Allow counting in CTTA 4 bit 3: 1b = Allow reset of CTTA 4 bits 2-1: RFU (00b) ***Note:*** *If the 'Do not reset CTTA during GENERATE AC' bit af the ADA has the value 1b, bits 6 & 3 should be set to 0b for all profiles.* Byte 8 (CTC 3 & CTC 4 controls): ***Note:*** *CTC = Consecutive Transaction Counter* bit 8: 1b = Check limits for CTC 3 bit 7: 1b = Allow counting in CTC 3 bit 6: 1b = Allow reset for CTC 3 bit 5: 1b = Check limits for CTC 4 bit 4: 1b = Allow counting in CTC 4 bit 3: 1b = Allow reset for CTC 4 bits 2-1: RFU (00b) *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (117 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Control x (continued)				Byte 9 (CTCI 3 & CTCI 4 controls): ***Note:*** *CTCI = Consecutive Transaction Counter International* bit 8: 1b = Check limits for CTCI 3 bit 7: 1b = Allow counting in CTCI 3 bit 6: 1b = Allow reset for CTC 3 bit 5: 1b = Check limits for CTCI 4 bit 4: 1b = Allow counting in CTCI 4 bit 3: 1b = Allow reset for CTC 4 bits 2-1: RFU (00b) Byte 10 (CTCIC 3 & CTCIC 4 controls): ***Note:*** *CTCIC = Consecutive Transaction Counter International Country* bit 8: 1b = Check limits for CTCIC 3 bit 7: 1b = Allow counting in CTCIC 3 bit 6: 1b = Allow reset for CTCIC 3 bit 5: 1b = Check limits for CTCIC 4 bit 4: 1b = Allow counting in CTCIC 4 bit 3: 1b = Allow reset for CTCIC 4 bits 2-1: RFU (00b) *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (118 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Control x (continued)				Byte 11 (Contactless controls): ***Note:*** *CLTC = Contactless Transaction Counter* bit 8: 1b = Check limits for VLP Available Funds bit 7: 1b = Allow reset of VLP Available Funds ***Note:*** *If the 'Do not reset VLP Available Funds during GENERATE AC' bit af the ADA has the value 1b, this bit should be set to 0b for all profiles.* ***Note:*** *bits 8-7 are RFU if the* VLP Available Funds *is not supported* bit 6: 1b = Check limits for CLTC bit 5: 1b = Allow reset of CLTC ***Note:*** *bits 6-5 are RFU if the CLTC is not supported* bits 4-1: RFU (0000b)
Profile Controls Template F: b T: 'BF59' L: var S: Card	C If Profiles Functionality is supported	Visa proprietary data template that contains the TLV-coded values for the Profile Controls.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	The following context-specific tags are defined in this specification for the Profile Controls Template: 'DF1x': Profile Control x

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (119 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Identifier (Profile ID) F: b T: – L: 1 S: Card	O	Identifies the Profile to be used in processing the transaction. The Profile ID is the output of the Profile Selection Algorithm and determines which Profile Control x is to be used to configure application data and behavior for transactions that use the profile.	UC: Transient IU: N R: N	Values are: '01' = Use Profile Control 1 '02' = Use Profile Control 2 '03' = Use Profile Control 3 '04' = Use Profile Control 4 '7F' = Reject GET PROCESSING OPTIONS command (no valid profile for the transaction),
Profile Selection Diversifier (PSD) **F: b** T: – L: 1 S: Card	C If profiles Functionality is supported	Identifies application- or transaction-specific internal card data that may be used in choosing the Profile. If there is no internal card data available for use in choosing a Profile, the default value for the PSD shall be '00'.	UC: Transient IU: N R: N	The coding of the PSD is at the discretion of the card manufacturer. Examples of internal card data that might be useful for choosing a Profile include: • on a multi-application card, which AID was used to select the application • on a dual-interface card, which physical interface (contact or contactless) is used for the transaction

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (120 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Selection Entry x F: b T: – L: var. S: Card	C If profiles Functionality is supported	Identifies record x in the Profile Selection File. The Profile Selection Entry x contains the logic for one step in the Profile Selection algorithm personalized by the issuer.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	Byte 1: Entry Length Byte 2: Position in Profile Selection Input Data Byte 3: Block Length Byte 4: Number of Blocks Byte 5 to n-3: Comparison Blocks: • Bit Mask • Comparison Value(s) x Byte n-2: Check Type Byte n-1: Positive Action Byte n: Negative Action
Profile Selection File F: b T: – L: var. S: Card	C If Profiles Functionality is supported	The file that contains the the rules personalized by the issuer for the simple logic the application uses to choose the Profile for a transaction. Each record in the file is a Profile Selection Entry x.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (121 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Profile Selection File Entry F: b T: 'DF02' in 'BF5B' L: 1 S: Card	C If Profiles Functionality is supported	Identifies the SFI of the file containing the Profile Selection Entries which are used to choose the Profile for a transaction.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	bits 8-4 = SFI containing the Profile Selection File ***Note:*** *To avoid conflict with possible Visa-defined uses of SFIs in the range 11-20, issuers should personalize the Profile Selection File in an SFI in the range 21-30.* bits 3-1= Number of records (Profile Selection Entries) in the Profile Selection File
Profile Selection Input Data **F: b** T: – L: var. S: Card and Terminal	C If profiles Functionality is supported	Identifies the data used as input for processing the profile selection logic using each Profile Selection Entry. Constructed from the Profile Selection Diversifier (determined by internal application processing) and value (obtained from the terminal) for the terminal data elements with a tag and length listed in the PDOL.	UC: Transient IU: N R: N	Byte 1: Profile Selection Diversifier Byte 2-n: GET PROCESSING OPTIONS command data (excluding the '83' template tag).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (122 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Proprietary Application Identifier Extensions (PIX) F: b T: – L: 0–11 S: Card	R	Portion of the card's Application Identifier (AID) which Identifies the Application Provider's specific application according to ISO/IEC 7816-5.	UC: Unchanging IU: N R: READ RECORD, SELECT	The currently assigned global Visa PIXs used for VSDC are: '1010' – Visa Debit or Credit '2010' – Electron '3010' – Interlink '8010' – PLUS
Proprietary Application Identifier Extensions (PIX) F: b T: Part of '9F06' L: 0-11 S: Terminal	R	As part of the terminal's Application Identifier (AID), identifies the application within the application provider (payment system).	n/a	
Proprietary Authentication Data F: b T: Part of '91' L: 1-8 S: Terminal	O Passed from issuer through terminal	Optional part of Issuer Authentication Data (IAuD) sent by the issuer in the online response for CVN 18.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (123 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Reference PIN F: b T: – L: 8 S: Card	C If offline PIN supported	Visa proprietary data element containing the PIN personalized in the card by the issuer.	UC: Modifiable IU: PIN CHANGE/ UNBLOCK R: N B: Backup Secret	
Registered Application Provider Identifier (RID) F: b T: – L: 5 S: Card	R	Portion of the Application Identifier (AID) which identifies the Application Provider according to ISO/IEC 7816-5.	UC: Unchanging IU: N R: READ RECORD, SELECT	Visa's RID is 'A000000003'.
Registered Application Provider Identifier (RID) F: b T: Part of '9F06' L: 5 S: Terminal	R	Portion of the Application Identifier (AID) which identifies the Application Provider according to ISO/IEC 7816-5.	n/a	Visa's RID is 'A000000003'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (124 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Response Message Template Format 1 F: var. T: '80' L: var. S: Card	O	Contains the data objects (without tags and lengths) returned by the ICC in response to a command. ***Note:*** *This template format cannot be used for CDA.*	UC: Transient IU: N R: GENERATE AC, GET PROCESSING OPTIONS, INTERNAL AUTHENTICATE	
Response Message Template Format 2 F: var. T: '77' L: var. S: Card	C If CDA is supported O If CDA is not supported	Contains the data objects (with tags and lengths) returned by the ICC in response to a command. ***Note:*** *This template format must be used for CDA.*	UC: Transient IU: N R: GENERATE AC, GET PROCESSING OPTIONS, INTERNAL AUTHENTICATE	
Service Code F: n 3 T: '5F30' L: 2 S: Card	O	Service code as defined on magnetic stripe tracks 1 and 2 according to ISO/IEC 7813.	UC: Unchanging IU: N R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (125 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Short File Identifier (SFI) F: b 8 T: '88' L: 1 S: Card	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.	UC: Unchanging IU: N R: SELECT	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} S: Card	C If DDA or CDA is supported	Dynamic digital signature generated by the card and validated by the terminal during DDA and CDA.	UC: Transient IU: N R: INTERNAL AUTHENTICATE	
Signed Static Application Data (SAD) F: b T: '93' L: N_I S: Card	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.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (126 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Static Data Authentication Failure Indicator F: b 1 T: – L: – S: Card	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.	UC: Persistent IU: N R: N B: Backup or default to 0b	bit 1: 1b = Offline static data authentication failed on last transaction and transaction declined offline Set to 1b during Offline Data Authentication if SDA fails and transaction is declined offline. Reset to 0b if online transaction (either approved or declined) and Issuer Authentication requirements are met
Static Data Authentication Tag List F: – T: '9F4A' L: var. S: Card	C If offline data authentication is supported	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.	UC: Unchanging IU: N R: READ RECORD	The SDA Tag List may not contain tags other than the tag for Application Interchange Profile (AIP).
Target Percentage to be Used for Random Selection F: – T: – L: – S: Terminal	C If online/offline terminal	Value used in terminal risk management for random transaction selection.	n/a	Visa may establish a range of values.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (127 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Action Code—Default F: b 40 T: – L: 5 S: Terminal	C If offline capable terminal	Specifies payment system conditions that cause a transaction to be declined if it might have been approved online, but the terminal is unable to process the transaction online.	n/a	Bit assignments are identical to those for Terminal Verification Results (TVR). The permissible values for the TAC-Default in this version of VIS is are shown in the *Visa Transaction Acceptance Device Requirements*.
Terminal Action Code—Denial F: b 40 T: – L: 5 S: Terminal	C If offline capable terminal	Specifies payment system conditions that cause the decline of a transaction without attempting to go online.	n/a	Bit assignments are identical to those for Terminal Verification Results (TVR). The permissible values for the TAC-Denial in this version of VIS is are shown in the *Visa Transaction Acceptance Device Requirements*.
Terminal Action Code—Online F: b 40 T: – L: 5 S: Terminal	C If online/offline terminal	Specifies payment system conditions that cause a transaction to be transmitted online.	n/a	Bit assignments are identical to those for Terminal Verification Results (TVR). The permissible values for the TAC-Online in this version of VIS is are shown in the *Visa Transaction Acceptance Device Requirements*.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (128 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Capabilities F: b 24 T: '9F33' L: 3 S: Terminal	R	Indicates the card data input, CVM, and security capabilities of the terminal.	n/a	Byte 1 (Card Data Input Capability): bit 8: 1b = Manual key entry bit 7: 1b = Magnetic stripe bit 6: 1b = IC with contacts bits 5-1: RFU (00000b) Byte 2 (CVM Capability): bit 8: 1b = Plaintext PIN for offline ICC verification bit 7: 1b = Enciphered PIN for online verification bit 6: 1b = Signature (paper) bit 5: 1b = Enciphered PIN for offline verification bit 4: 1b = No CVM Required bits 3-1: RFU (000b) Byte 3 (Security Capability): bit 8: 1b = SDA bit 7: 1b = DDA bit 6: 1b = Card capture bit 5: RFU (0b) bit 4: 1b = CDA bits 3-1: RFU (000b)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (129 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Country Code F: n 3 T: '9F1A' L: 2 S: Terminal	R	Indicates the country of the terminal represented according to ISO 3166.	n/a	
Terminal Floor Limit F: b 32 T: '9F1B' L: 4 S: Terminal	C if offline capable terminal	Indicates the floor limit in the terminal in conjunction with the AID.	n/a	
Terminal Identification F: an 8 T: '9F1C' L: 8 S: Terminal	R (at terminal or acquirer)	Designates the unique location of a terminal at a merchant.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (130 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Risk Management Data F: b 8-64 T: '9F1D' L: 1-8 S: Terminal	O	Application-specific value used by the card for risk management purposes.	n/a	
Terminal Type F: n 2 T: '9F35' L: 1 S: Terminal	R	Indicates the environment of the terminal, its communications capability, and its operational control.	n/a	Values are: '11' = Attended, online only, operated by financial institution '12' = Attended, offline with online capability, operated by financial institution '13' = Attended, offline only, operated by financial institution '14' = Unattended, online only, operated by financial institution '15' = Unattended, offline with online capability, operated by financial institution '16' = Unattended, offline only, operated by financial institution *- continues -*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (131 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Type (continued)				'21' = Attended, online only, operated by merchant '22' = Attended, offline with online capability, operated by merchant '23' = Attended, offline only, operated by merchant '24' = Unattended, online only, operated by merchant '25' = Unattended, offline with online capability, operated by merchant '26' = Unattended, offline only, operated by merchant '34' = Unattended, online only, operated by cardholder '35' = Unattended, offline with online capability, operated by cardholder '36' = Unattended, offline only, operated by cardholder

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (132 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Verification Results (TVR) F: b 40 T: '95' L: 5 S: Terminal	R	Status of the different functions as seen from the terminal. ***Note:*** *The issuer needs to set the 'Issuer Script processing failed after final GENERATE AC' bit to 0b prior to validating the Application Cryptogram.*	n/a	Byte 1 bit 8: 1b = Offline data authentication was not performed bit 7: 1b = SDA failed bit 6: 1b = ICC data missing bit 5: 1b = Card appears on terminal exception file bit 4: 1b = DDA failed bit 3: 1b = CDA failed bit 2: 1b = SDA selected bit 1: RFU (0b) Byte 2 bit 8: 1b = ICC and terminal have different application versions bit 7: 1b = Expired application bit 6: 1b = Application not yet effective bit 5: 1b = Requested service not allowed for card product bit 4: 1b = New card bits 3-1: RFU (000b)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (133 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Verification Results (TVR) (continued)				Byte 3 bit 8: 1b = Cardholder verification was not successful bit 7: 1b = Unrecognized CVM bit 6: 1b = PIN Try Limit exceeded bit 5: 1b = PIN entry required and PIN pad not present or not working bit 4: 1b = PIN entry required, PIN pad present, but PIN was not entered bit 3: 1b = Online PIN entered bits 2-1: RFU (00b) Byte 4 bit 8: 1b = Transaction exceeds floor limit bit 7: 1b = Lower consecutive offline limit ('9F14') exceeded bit 6: 1b = Upper consecutive offline limit ('9F23') exceeded bit 5: 1b = Transaction selected randomly for online processing bit 4: 1b = Merchant forced transaction online bits 3-1: RFU (000b)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (134 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Terminal Verification Results (TVR) (continued)				Byte 5 bit 8: 1b = Default TDOL used bit 7: 1b = Issuer Authentication was unsuccessful bit 6: 1b = Issuer Script processing failed before final GENERATE AC command bit 5: 1b = Issuer Script processing failed after final GENERATE AC command bits 4-1: RFU (0000b)
Threshold Value for Biased Random Selection F: – T: – L: – S: Terminal	C if online/offline terminal	Value used in terminal risk management for random transaction selection.	n/a	Visa may establish a range of values.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (135 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Track 1 Discretionary Data F: ans T: '9F1F' L: var. S: Card	O	Discretionary data from track 1 of the magnetic stripe according to ISO/IEC 7813. That is, if personalized for VIS, this data element contains the data in Track 1 that comes after the Service Code and before the End Sentinel.	UC: Modifiable IU: UPDATE RECORD (if update of the PVV is supported) R: READ RECORD	***Note:*** *The contents of this data element for VIS transactions is different from the content for VCPS transactions.* ***Note:*** *The maximum length of this data element is dependent on the length of other data that may be present in Track 1 data. See also the Visa Payment Systems Technology Manual for more information about the length limitations for Track 1 Discretionary Data.*
Track 2 Discretionary Data F: cn T: '9F20' L: var. S: Card	not applicable	Discretionary data from track 2 of the magnetic stripe according to ISO/IEC 7813. Not used in this version of VIS.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (136 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Track 2 Equivalent Data F: b T: '57' L: var. up to 19	R	Contains the data elements of the track 2 according to the ISO/IEC 7813, excluding start sentinel, end sentinel, and LRC, as follows: n, var. up to 19 — Primary Account Number 1 — Field Separator ('D') n4 — Expiration Date (YYMM) n3 — Service Code 0 or n 5 — PIN Verification Field n, var. — Discretionary Data (defined by individual payment systems) hex. — Pad with 'F' if needed to ensure whole bytes.	UC: Modifiable IU: UPDATE RECORD (if update of the PVV is supported) R: READ RECORD	***Note:*** *The contents of this data element for VIS transactions is different from the content for VCPS transactions.*
Transaction Amount F: n12 T: – L: 6 S: Terminal	R	Clearing amount of the transaction, including tips and other adjustments.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (137 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Transaction Certificate Data Object List (TDOL) F: b T: '97' L: var. up to 252 S: Card	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 D do not use the TDOL.	UC: Unchanging IU: N R: READ RECORD	
Transaction Certificate (TC) Hash Value F: b 160 T: '98' L: 20 S: Terminal	O	Result of a hash function specified in *EMV Book 3*, Section 5.2.2. The cryptogram versions described in Appendix D do not use the TC Hash Value.	n/a	
Transaction Currency Code F: n 3 T: '5F2A' L: 2 S: Terminal	R	Indicates the currency code of the transaction according to ISO 4217. The implied exponent is indicated by the minor unit of currency associated with the Transaction Currency Code in ISO 4217.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (138 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Transaction Currency Exponent F: n 1 T: '5F36' L: 1 S: Terminal	R	Indicates the implied position of the decimal point from the right of the transaction amount represented according to ISO 4217.	n/a	
Transaction Date F: n 6 YYMMDD T: '9A' L: 3 S: Terminal	R	Local date that the transaction was authorized.	n/a	
Transaction Personal Identification Number (PIN) Data F: b T: '99' L: var. S: Terminal	C If PIN supported	Data entered by the cardholder for the purpose of PIN verification.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (139 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Transaction Reference Currency Code F: n 3 T: '9F3C' L: 2 S: Terminal	not applicable	Code defining the common currency used by the terminal in case the Transaction Currency Code is different from the Application Currency Code. This data object is not used in this version of VIS.	n/a	
Transaction Reference Currency Conversion F: n 8 T: – L: 4 S: Terminal	not applicable	Factor used in the conversion from the Transaction Currency Code to the Transaction Reference Currency Code. This data object is not used in this version of VIS.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (140 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Transaction Reference Currency Exponent F: n 1 T: '9F3D' L: 1 S: Terminal	not applicable	Indicates the implied position of the decimal point from the right of the Transaction Amount, with the reference currency code represented according to ISO 4217. This data object is not used in this version of VIS.	n/a	
Transaction Sequence Counter F: n 4-8 T: '9F41' L: 2-4 S: Terminal	R	Counter maintained by the terminal that is incremented by one for each transaction.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (141 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Transaction Status Information (TSI) F: b 16 T: '9B' L: 2 S: Terminal	R	Indicates the functions performed in a terminal.	n/a	Byte 1: bit 8: 1b = Offline data authentication was performed bit 7: 1b = Cardholder verification was performed bit 6: 1b = Card risk management was performed bit 5: 1b = Issuer Authentication was performed bit 4: 1b = Terminal risk management was performed bit 3: 1b = Issuer Script processing was performed bits 2-1: RFU (00b) Byte 2: RFU ('00')
Transaction Time F: n 6 HHMMSS T: '9F21' L: 3 S: Terminal	R	Local time that the transaction was authorized.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (142 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Transaction Type F: n 2 T: '9C' L: 1 S: Terminal	R	Indicates the type of financial transaction, represented by the values of the first two digits of Processing Code as defined by Visa.	n/a	
Unique Data Encipherment DEA Key A (ENC UDK A) **F: b 64** **T: –** **L: 8** S: Card	C If post-issuance updates to confidential data (such as Reference PIN) 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. ***Note:*** *What VIS calls the Unique Data Encipherment DEA Key, in EMV is called the Encipherment Master Key,* MK_{ENC}.	UC: Unchanging IU: N R: N Secret	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (143 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Unique Data Encipherment DEA Key B (ENC UDK B) **F: b 64** T: – L: 8 S: Card	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. ***Note:*** *What VIS calls the Unique Data Encipherment DEA Key, in EMV is called the Encipherment Master Key,* MK_{ENC}.	UC: Unchanging IU: N R: N Secret	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (144 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Unique DEA Key A (UDK A) F: b 64 T: – L: 8 S: Card	R	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. ***Note:*** *What VIS calls the UDK, in EMV is called the ICC Master Key, MK_{AC}.*	UC: Unchanging IU: N R: N Secret	
Unique DEA Key B (UDK B) F: b 64 T: – L: 8 S: Card	R	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. ***Note:*** *What VIS calls the UDK, in EMV is called the ICC Master Key, MK_{AC}.*	UC: Unchanging IU: N R: N Secret	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (145 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Unique Message Authentication Code (MAC) DEA Key A (MAC UDK A) F: b 64 T: – L: 8 S: Card	C If Issuer Script using secure messaging is 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. ***Note:*** *What VIS calls the MAC UDK, in EMV is called the MAC Master Key, MK_{MAC}.*	UC: Unchanging IU: N R: N Secret	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (146 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Unique Message Authentication Code (MAC) DEA Key B (MAC UDK B) F: b 64 T: – L: 8 S: Card	C If Issuer Script using secure messaging is 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. ***Note:*** *What VIS calls the MAC UDK, in EMV is called the MAC Master Key, MK_{MAC}.*	UC: Unchanging IU: N R: N Secret	
Unpredictable Number F: b 32 T: '9F37' L: 4 S: Terminal	R	Value to provide variability and uniqueness to the generation of the application cryptogram.	n/a	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (147 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
Upper Consecutive Offline Limit (UCOL) F: b 8 T: '9F23' L: 1 S: Card	C If terminal velocity check (LCOL or UCOL) or terminal new card 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.	UC: Modifiable IU: UPDATE RECORD R: READ RECORD B: Backup	
Visa Discretionary Data F: b 56 T: Part of '9F10' L: 7 S: Card	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.	UC: Dynamic IU: PUT DATA to '9F10' (only the DKI and CVN may be modified) R: GENERATE AC	

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (148 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
VLP Available Funds F: n 12 T: '9F79' or 'DF51' in 'BF55' L: 6 S: Card	C If supported for contactless velocity checking	Visa proprietary data element that provides a counter that may be decremented by the transaction amount for qVSDC offline approved contactless transactions.	UC: Dynamic IU: PUT DATA R: GET DATA (SD), GENERATE AC (if included in the Issuer Discretionary Data Option supported as described in Appendix J) B: Backup or default to zero	Initialized to a value of zero if VLP Funds Limit is personalized. Issuers may personalize the VLP Available Funds with another initial value. Decremented during offline approved contactless transactions Reset to VLP Funds Limit: • if online transaction, final cryptogram is a TC, Issuer Authentication requirements are met, and ADA allows reset during GENERATE AC • if VLP Funds Limit is updated by an Issuer Script and ADA only allows reset with an Issuer Script.
VLP Funds Limit F: n 12 T: '9F77' or 'DF71' in 'BF55' L: 6 S: Card	C If supported for contactless velocity checking	A Visa proprietary data element that provides the issuer limit for VLP Available Funds, and is the value to which VLP Available Funds is reset after an online approved transaction.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-1: Data Element Descriptions (149 of 149)

Name (Format; Tag/Template; Length; Source)	Requirement	Description	Update Capability, Update, Retrieval, Backup, Secret	Values
VLP Reset Threshold F: n 12 T: '9F6D' or 'DF61' in 'BF55' L: 6 S: Card	O If supported for contactless velocity checking	A Visa proprietary data element specifying the minimum value to which the VLP Available Funds is allowed to be decremented before the card requests online processing.	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	
VLP Single Transaction Limit F: n 12 T: '9F78' or 'DF41' in 'BF55' L: 6 S: Card	C If supported for contactless velocity checking	A Visa proprietary data element indicating the maximum amount allowed for a single qVSDC offline contactless transaction	UC: Modifiable IU: PUT DATA R: GET DATA (SD)	Set during personalization.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

A.2 Data Element Tags

The tags allocated to the card, issuer, and terminal data elements are shown in Table A-2.

For data elements that use a tag that only has meaning within the context of a template, the Template column indicates the template in which the data element.

Table A-2: Data Element Tags (1 of 9)

Template	Tag	Data Element	Source
	'42'	Issuer Identification Number (IIN)	Card
	'4F'	Application Identifier (AID)	Card
	'50'	Application Label	Card
	'57'	Track 2 Equivalent Data	Card
	'5A'	Application PAN	Card
	'5F20'	Cardholder Name	Card
	'5F24'	Application Expiration Date	Card
	'5F25'	Application Effective Date	Card
	'5F28'	Issuer Country Code	Card
	'5F2A'	Transaction Currency Code	Terminal
	'5F2D'	Language Preference	Card
	'5F30'	Service Code	Card
	'5F34'	Application PAN Sequence Number	Card
	'5F36'	Transaction Currency Exponent	Terminal
	'5F50'	Issuer URL *(not used)*	Card
	'5F53'	Issuer Identification Number (IIN)	Card
	'5F54'	Bank Identifier Code (BIC)	Card
	'5F55'	Issuer Country Code (alpha2)	Card

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (2 of 9)

Template	Tag	Data Element	Source
	'5F56'	Issuer Country Code (alpha3)	Card
	'5F57'	Account Type	Terminal
	'61'	Application Template	Card
	'6F'	File Control Information (FCI) Template	Card
	'71'	Issuer Script Template 1	Issuer
	'72'	Issuer Script Template 2	Issuer
	'73'	Directory Discretionary Template	Card
	'77'	Response Message Template Format 2	Card
	'80'	Response Message Template Format 1	Card
	'81'	Amount, Authorized (binary) *(not used)*	Terminal
	'82'	Application Interchange Profile (AIP)	Card
	'83'	Command Template	Terminal
	'84'	Dedicated File (DF) Name	Card
	'86'	Issuer Script Command	Issuer
	'87'	Application Priority Indicator	Card
	'88'	Short File Identifier (SFI)	Card
	'89'	Authorization Code	Issuer
	'8A'	Authorization Response Code	Issuer/ Terminal
	'8C'	Card Risk Management Data Object List 1 (CDOL1)	Card
	'8D'	Card Risk Management Data Object List 2 (CDOL2)	Card

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (3 of 9)

Template	Tag	Data Element	Source
	'8E'	Cardholder Verification Method (CVM) List	Card
	'8F'	Certificate Authority Public Key Index (PKI)	Card
	'90'	Issuer PK Certificate	Card
	'91'	Issuer Authentication Data	Issuer
	'92'	Issuer PK Remainder	Card
	'93'	Signed Static Application Data	Card
	'94'	Application File Locator (AFL)	Card
	'95'	Terminal Verification Results	Terminal
	'97'	Transaction Certificate Data Object List (TDOL)	Card
	'98'	Transaction Certificate (TC) Hash Value	Terminal
	'99'	Transaction PIN	Terminal
	'9A'	Transaction Date	Terminal
	'9B'	Transaction Status Information (TSI)	Terminal
	'9C'	Transaction Type	Terminal
	'9D'	Directory Definition File (DDF) Name	Card
	'9F01'	Acquirer Identifier	Terminal
	'9F02'	Amount, Authorized (Numeric)	Terminal
	'9F03'	Amount, Other (Numeric)	Terminal
	'9F04'	Amount, Other (Binary) *(not used)*	Terminal
	'9F05'	Application Discretionary Data	Card
	'9F06'	Application Identifier (AID)	Terminal

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (4 of 9)

Template	Tag	Data Element	Source
	'9F07'	Application Usage Control	Card
	'9F08'	Application Version Number	Card
	'9F09'	Application Version Number	Terminal
	'9F0A'	Application Selection Registered Proprietary Data (ASRPD)	Card
	'9F0B'	Cardholder Name—Extended	Card
	'9F0D'	Issuer Action Code—Default	Card
	'9F0E'	Issuer Action Code—Denial	Card
	'9F0F'	Issuer Action Code—Online	Card
	'9F10'	Issuer Application Data	Card
	'9F11'	Issuer Code Table Index	Card
	'9F12'	Application Preferred Name	Card
	'9F13'	Last Online ATC Register	Card
	'9F14'	Lower Consecutive Offline Limit (Terminal Check)	Card
	'9F15'	Merchant Category Code	Terminal
	'9F16'	Merchant Identifier	Terminal
	'9F17'	PIN Try Counter	Card
	'9F18'	Issuer Script Identifier	Issuer
	'9F1A'	Terminal Country Code	Terminal
	'9F1B'	Terminal Floor Limit	Terminal
	'9F1C'	Terminal Identification	Terminal

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (5 of 9)

Template	Tag	Data Element	Source
	'9F1D'	Terminal Risk Management Data	Terminal
	'9F1E'	Interface Device (IFD) Serial Number	Terminal
	'9F1F'	Track 1 Discretionary Data	Card
	'9F20'	Track 2 Discretionary Data *(not used)*	Card
	'9F21'	Transaction Time	Terminal
	'9F22'	Certificate Authority Public Key Index (PKI)	Terminal
	'9F23'	Upper Consecutive Offline Limit (Terminal Check)	Card
	'9F24'	Payment Account Reference (PAR)	Card
	'9F26'	Application Cryptogram (AC)	Card
	'9F27'	Cryptogram Information Data	Card
	'9F2D'	ICC PIN Encipherment Public Key Certificate	Card
	'9F2E'	ICC PIN Encipherment Public Key Exponent	Card
	'9F2F'	ICC PIN Encipherment Public Key Remainder	Card
	'9F32'	Issuer PK Exponent	Card
	'9F33'	Terminal Capabilities	Terminal
	'9F34'	Cardholder Verification Method (CVM) Results	Terminal
	'9F35'	Terminal Type	Terminal
	'9F36'	Application Transaction Counter (ATC)	Card
	'9F37'	Unpredictable Number	Terminal
	'9F38'	Processing Options Data Object List (PDOL)	Card
	'9F3A'	Amount, Reference Currency (Binary) *(not used)*	Terminal

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (6 of 9)

Template	Tag	Data Element	Source
	'9F3B'	Application Reference Currency *(not used)*	Card
	'9F3C'	Transaction Reference Currency Code *(not used)*	Terminal
	'9F3D'	Transaction Reference Currency Exponent *(not used)*	Terminal
	'9F40'	Additional Terminal Capabilities	Terminal
	'9F41'	Transaction Sequence Counter	Terminal
	'9F42'	Application Currency Code	Card
	'9F43'	Application Reference Currency Exponent *(not used)*	Card
	'9F44'	Application Currency Exponent	Card
	'9F45'	Data Authentication Code	Card
	'9F46'	ICC Public Key Certificate	Card
	'9F47'	ICC Public Key Exponent	Card
	'9F48'	ICC Public Key Remainder	Card
	'9F49'	Dynamic Data Authentication Data Object List (DDOL)	Card
	'9F4A'	Static Data Authentication Tag List	Card
	'9F4B'	Signed Dynamic Application Data	Card
	'9F4C'	Integrated Circuit Card (ICC) Dynamic Number	Card
	'9F4D'	Log Entry	Card
	'9F4E'	Merchant Name and Location	Terminal or Acquirer
	'9F4F'	Log Format	Card
	'9F51'	Application Currency Code	Card

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (7 of 9)

Template	Tag	Data Element	Source
	'9F52'	Application Default Action (ADA)	Card
	'9F53'	Consecutive Transaction Counter International Limit (CTCIL)	Card
	'9F54'	Cumulative Total Transaction Amount Limit (CTTAL)	Card
	'9F56'	Issuer Authentication Indicator	Card
	'9F57'	Issuer Country Code	Card
	'9F58'	Consecutive Transaction Counter Limit (CTCL)	Card
	'9F59'	Consecutive Transaction Counter Upper Limit (CTCUL)	Card
	'9F5B'	Issuer Script Results	Terminal
	'9F5C'	Cumulative Total Transaction Amount Upper Limit (CTTAUL)	Card
	'9F5D'	Available Offline Spending Amount	Card
	'9F5E'	Consecutive Transaction International Upper Limit (CTIUL)	Card
	'9F6D'	VLP Reset Threshold	Card
	'9F68'	Card Additional Processes	Card
	'9F72'	Consecutive Transaction Counter International Country Limit (CTCICL)	Card
	'9F73'	Currency Conversion Parameters	Card
	'9F77'	VLP Funds Limit	Card
	'9F78'	VLP Single Transaction Limit	Card
	'9F79'	VLP Available Funds	Card

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (8 of 9)

Template	Tag	Data Element	Source
	'A5'	File Control Information (FCI) Proprietary Template	Card
	'BF0C'	File Control Information (FCI) Issuer Discretionary Data	Card
'BF55'		Contactless Counters Template	Card
'BF56'		Counters Data Template	Card
'BF57'		International Counters Data Template	Card
'BF58'		Amounts Data Template	Card
'BF59'		Profile Controls Template	Card
'BF5A'		AIP/AFL Entries Template	Card
'BF5B'		Application Internal Data Template	Card
'BF55'	'DF11'	Contactless Transaction Counter (CLTC)	Card
'BF55'	'DF21'	Contactless Transaction Counter Lower Limit (CLTCLL)	Card
'BF55'	'DF31'	Contactless Transaction Counter Upper Limit (CLTCUL)	Card
'BF55'	'DF41'	VLP Single Transaction Limit	Card
'BF55'	'DF51'	VLP Available Funds	Card
'BF55'	'DF61'	VLP Reset Threshold	Card
'BF55'	'DF71'	VLP Funds Limit	Card
'BF56'	'DF1x'	Consecutive Transaction Counter (CTC x)	Card
'BF56'	'DF2x'	Consecutive Transaction Counter Limit (CTCL x)	Card
'BF56'	'DF3x'	Consecutive Transaction Counter Upper Limit (CTCUL x)	Card

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table A-2: Data Element Tags (9 of 9)

Template	Tag	Data Element	Source
'BF57'	'DF1x'	Consecutive Transaction Counter International (CTCI x)	Card
'BF57'	'DF2x'	Consecutive Transaction Counter International Limit (CTCIL x)	Card
'BF57'	'DF3x'	Consecutive Transaction International Upper Limit (CTIUL x)	Card
'BF57'	'DF5x'	Consecutive Transaction Counter International Country (CTCIC x)	Card
'BF57'	'DF6x'	Consecutive Transaction Counter International Country Limit (CTCICL x)	Card
'BF58'	'DF1x'	Cumulative Total Transaction Amount (CTTA x)	Card
'BF58'	'DF2x'	Cumulative Total Transaction Amount Limit (CTTAL x)	Card
'BF58'	'DF3x'	Cumulative Total Transaction Amount Upper Limit (CTTAUL x)	Card
'BF59'	'DF1x'	Profile Control x	Card
'BF5A'	'DF1x'	AIP/AFL Entry x	Card
'BF5B'	'DF01'	Application Capabilities	Card
'BF5B'	'DF02'	Profile Selection File Entry	Card

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

B Secure Messaging

Secure messaging shall be performed as described in *EMV 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).

This appendix includes the following sections:

B.1 Secure Messaging Format

B.2 Message Integrity and Authentication (MACing)

B.3 Data Confidentiality

B.4 Secure Messaging Session Key Generation

B.5 Secure Messaging Impact on Command Formats

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

B.1 Secure Messaging Format

The secure messaging format defined in this specification is compliant with ISO/IEC 7816-4. Secure messaging is indicated for an Issuer Script Command when the second nibble of the CLA byte is equal to '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 or 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. 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 '00 00 00 00 00 00 00 00'.

   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.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 or 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 or 8; it is never zero.*

   – Last ATC (for Issuer Script processing, this is the ATC transmitted in the request message)
   – An 8-byte value as follows:
     - If *either* the 'Use Issuer Script MAC Chaining Option' bit of the Application Default Action (ADA) has the value 0b, *or* this is the first issuer script command received by the application for the current ATC value; then use the Application Cryptogram returned in the response to the first.GENERATE AC command (the one transmitted in the online authorization request message).
     - If the 'Use Issuer Script MAC Chaining Option' bit of the Application Default Action (ADA) has the value 1b *and* this is not the first issuer script command for the current transaction (ATC value); then use the full 8-byte MAC of the preceding Issuer Script command (as computed by this MAC algorithm, prior to any truncation that occurs when shorter MACs are transmitted).
   – 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, then an additional 8-byte data block is concatenated to the right of the last data block as follows: '80 00 00 00 00 00 00 00'. Proceed to step 5.

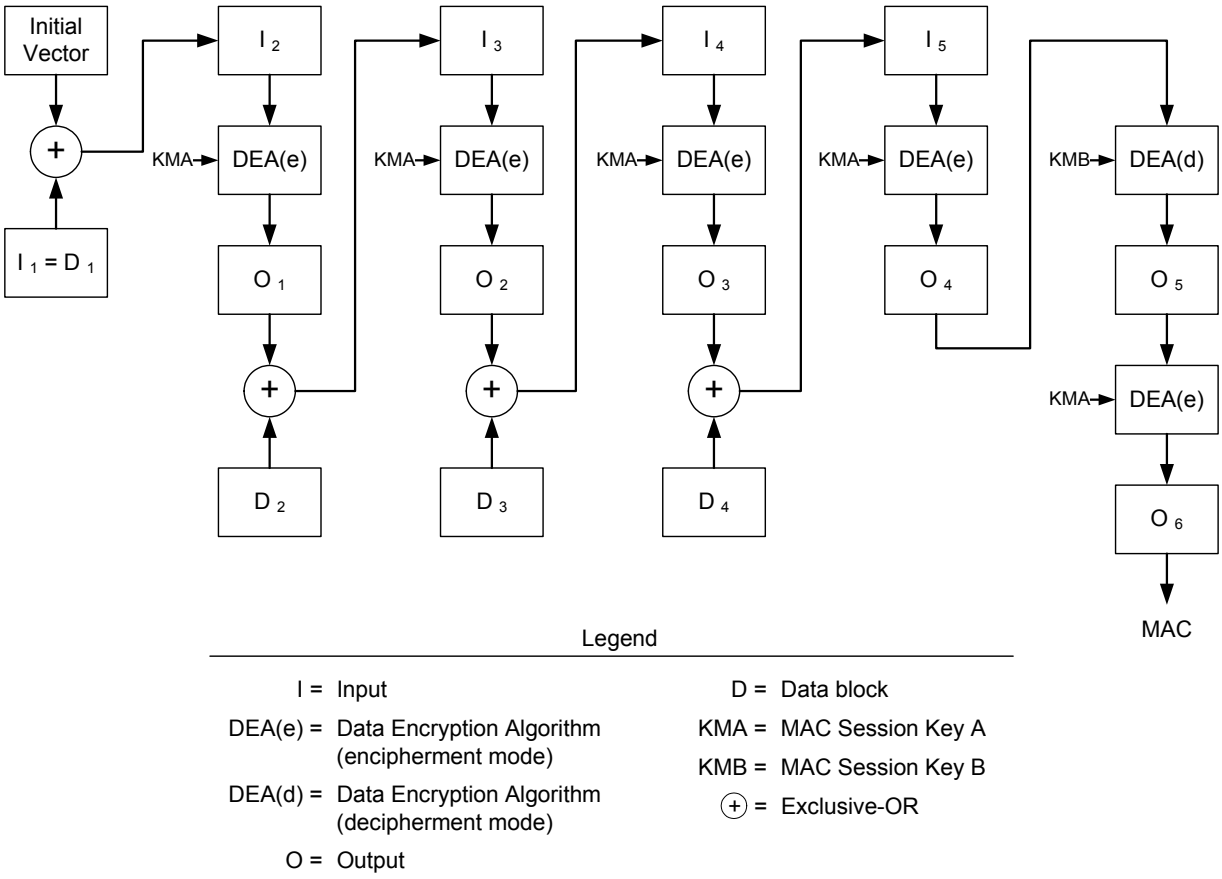
   If the last data block is less than 8 bytes in length, then it is padded to the right with a 1-byte '80'. If the last data block is now 8 bytes in length, proceed to step 5. If the last data block is still less than 8 bytes in length, then it is right filled with 1-byte blocks of '00' until it is 8 bytes in length.
5. The data blocks are enciphered using the MAC Session Key, which is generated as described in section B.4.

   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.)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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. 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)

The entire block of data is then enciphered using the data encipherment technique described in section B.3.3.

B.3.3 Data Encipherment Calculation

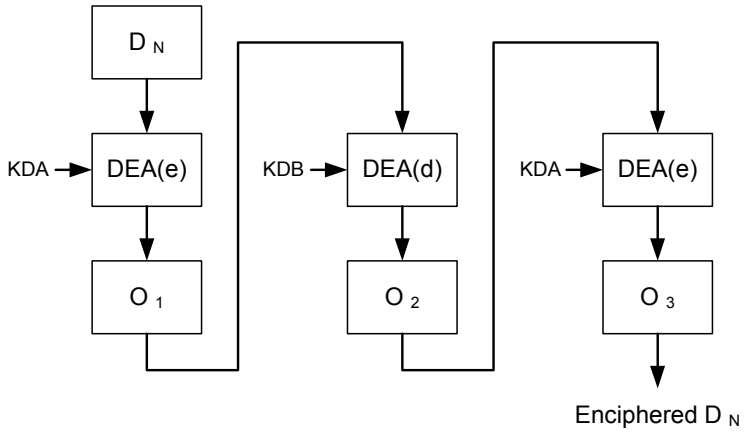
Data encipherment occurs prior to generation of the MAC. The data encipherment technique is as follows:

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, then it is padded to the right with '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, then it is right filled with 1-byte blocks of '00' until it is 8 bytes.
4. Each data block is enciphered using the Data Encipherment Session Key generated as described in section B.4.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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



Legend

DEA(e) =	Data Encryption Algorithm (encipherment mode)	D =	Data block
DEA(d) =	Data Encryption Algorithm (decipherment mode)	KDA =	Data Encipherment Session Key A
O =	Output	KDB =	Data Encipherment Session Key B

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

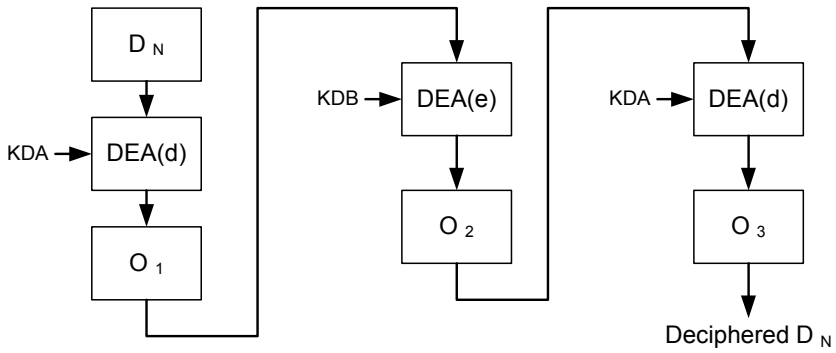
B.3.4 Data Decipherment Calculation

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.

   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



Legend:

DEA(e) =	Data Encryption Algorithm (encipherment mode)	D =	Data block
DEA(d) =	Data Encryption Algorithm (decipherment mode)	KDA =	Data Encipherment Session Key A
O =	Output	KDB =	Data Encipherment Session Key B

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).
3. Since LD indicates the length of the plaintext data, it is used to recover the plaintext data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

B.4 Secure Messaging Session Key Generation

This version of VIS supports the following methods for the generation of the MAC and data encipherment session keys:

- the exclusive-OR (XOR) based derivation method defined in section B.4.1. This method can be used only in combination with CVN 10 and CVN 18.

  Note: *This was the only method defined in VIS 1.5.4 and earlier versions.*

- the EMV common session key derivation method defined in section D.7.2. This method can be used only in combination with CVN '22'."

  Note: *This method was introduced in VIS version 1.6.*

In the following sections, the two methods are defined using the generic terms session Key A and session Key B.

B.4.1 XOR Session Key Generation

Note: *The following session key derivation method is identical to the method defined in VIS 1.5.4 and earlier versions.*

1. This method shall be used for secure messaging when performed in combination with CVN 10 and CVN 18.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 '00 00 00 00 00 00'. 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 'FF FF'. The inverted ATC is right-justified in an 8-byte field and the remaining 6 bytes are filled with '00 00 00 00 00 00'. Session Key B is generated by performing an exclusive-OR operation on Key B with the resulting 8-byte inverted ATC field.

B.4.2 EMV Common Session Key Generation

The EMV common session key derivation is described in section D.7.2. This method shall be used for secure messaging when performed in combination with CVN '22'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 generated Application Cryptogram (the one transmitted in the request message) is copied to a 8-byte field, where the third leftmost byte is replaced with the value ‘F0’. Session Key A is generated by performing a Triple DEA encipherment of this 8-byte field with the MAC UDK or ENC UDK.
3. The last generated ARQC (the one transmitted in the request message) is copied to a 8-byte field, where the third leftmost byte is replaced with the value ‘0F’. Session Key B is generated by performing a Triple DEA encipherment of this 8-byte field with the MAC UDK or ENC UDK.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 provides the information needed by issuers that wish to use secure messaging with commands not listed in , to implement the correct command APDU format.

Note: *In the EMV specifications, 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 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C Commands for Financial Transactions

This appendix lists the commands described in the functional chapters of this document and in *EMV Book 1*, section 11, and *EMV Book 3*, section 6.5. These commands are used to implement 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 implementation 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 *EMV Book 1*, section 11, and *EMV Book 3*, section 6.5.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

If an error occurred during MAC validation for an issuer script command, the card shall respond with SW1 SW2 = '6988' or '6987'. The card should respond with:

- SW1 SW2 = '6987' (Secure messaging data object missing) if the MAC is not present
- SW1 SW2 = '6988' (Secure messaging data object incorrect) if the MAC is incorrect.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.2 APPLICATION BLOCK Command—Response Application Protocol Data Units (APDUs)

The APPLICATION BLOCK command is a post-issuance command that invalidates the currently selected application.

The APPLICATION BLOCK command shall be performed as described in *EMV Book 3*, section 6.5.1.

The command data field shall contain the 4 or 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 a single 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 *VSDC Personalization Specification*.

Note: *During any subsequent Application Selection, the card does 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, then the card is required to return an AAC in response to a GENERATE AC command.*

C.2.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

If the P1 P2 parameters of the command have a value other than '0000', the card shall respond with an SW1 SW2 that indicates an error and should return SW1 SW2 = '6A81' (Function not supported).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.3 APPLICATION UNBLOCK Command—Response APDUs

The APPLICATION UNBLOCK command is a post-issuance command that reverses the blocking of an application that has not been permanently blocked.

The APPLICATION UNBLOCK command shall be performed as described in *EMV Book 3*, section 6.5.2.

The command data field shall contain the 4 or 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 *VSDC Personalization Specification*.

C.3.1 Processing State Returned in the Response Message

If the application is permanently blocked (for example, because the ATC has reached its limit or an application that was linked to this application for application blocking became permanently blocked), the card shall respond to the APPLICATION UNBLOCK command with SW1 SW2 = '6985'.

A successful execution of the command is coded by SW1 SW2 = '9000'.

If the P1 P2 parameters of the command have a value other than '0000', the card shall respond with an SW1 SW2 that indicates an error and should return SW1 SW2 = '6A81' (Function not supported).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.4 CARD BLOCK Command—Response APDUs

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

The CARD BLOCK command shall be performed as described in *EMV Book 3*, section 6.5.3.

Note: *The application continues processing the current transaction through completion, including any issuer script command processing. The card block becomes effective when a subsequent transaction attempts application selection.*

The command data field shall contain the 4 or 8 byte MAC generated using the Format 2 method. The MAC generation process is described in Appendix B, Secure Messaging.

C.4.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

If the P1 P2 parameters of the command have a value other than '0000', the card shall respond with an SW1 SW2 that indicates an error and should return SW1 SW2 = '6A81' (Function not supported).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.5 EXTERNAL AUTHENTICATE Command—Response APDUs

The EXTERNAL AUTHENTICATE command shall be performed as described in *EMV Book 3*, section 6.5.4. This command is used in performing online Issuer Authentication if Issuer Authentication is supported using the EXTERNAL AUTHENTICATE command.

The card permits 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 *EMV Book 3*, section 6.5.4, the first eight bytes contain the mandatory Authorization Response Cryptogram (ARPC), followed by an optional one to eight bytes.

In this version of VIS, the Issuer Authentication Data sent in the EXTERNAL AUTHENTICATE command shall consist of the following data; optional issuer data is not supported:

- ARPC
- ARPC Response Code

The mandatory algorithm for generating and verifying the ARPC is described in Appendix D, Authentication Data, Keys and Algorithms.

C.5.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

If the P1 P2 parameters of the command have a value other than '0000', the card shall respond with an SW1 SW2 that indicates an error and should return SW1 SW2 = '6A81' (Function not supported).

The card shall permit at most one EXTERNAL AUTHENTICATE command in a transaction. If the card receives more than one EXTERNAL AUTHENTICATE command for a single value of the ATC, then for the second and all subsequent EXTERNAL AUTHENTICATE commands the card shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied) and shall not perform Issuer Authentication.

If the card receives a delayed EXTERNAL AUTHENTICATE command after having performed Issuer Authentication as part of processing the second GENERATE AC command for the same transaction (same value of the ATC), the card shall not perform Issuer Authentication again as part of processing the EXTERNAL AUTHENTICATE command and shall respond to the EXTERNAL AUTHENTICATE command with SW1 SW2 = '6985' (Conditions of use not satisfied).

If the application is permanently blocked, then the card shall discontinue processing the command, shall not perform Issuer Authentication, and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.6 GENERATE APPLICATION CRYPTOGRAM (AC) Command—Response APDUs

The GENERATE APPLICATION CRYPTOGRAM (AC) command shall be performed as described in *EMV Book 3*, section 6.5.5. This command is used in generating the Authorization Request Cryptogram (ARQC), Transaction Certificate (TC), and Application Authentication Cryptogram (AAC).

The mandatory algorithm for generating the TC, AAC, and ARQC is described in Appendix D, Authentication Data, Keys and Algorithms.

If the response to the GENERATE AC command contains a dynamic signature, the card shall code the data field returned in the response according to Format 2 as described in *EMV Book 3*, section 6.5.5.4. Format 2 uses BER-TLV encoding for the data elements in the response. If the response is returned in an envelope, then the data returned shall be in the format shown in *EMV Book 2*, Table 20.

Otherwise (a dynamic signature is not being returned):

- Cards not capable of supporting the CDA feature shall code the data field returned in the response according to either Format 1 or Format 2 as described in *EMV Book 3*, section 6.5.5.4, which allows a card to transmit to the terminal a variable-length data object called the Issuer Application Data.
- Cards capable of supporting the CDA feature shall code the data field returned in the response according to Format 2 as discussed above.

In this version of VIS, 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.

C.6.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

For the error conditions shown in Table C-1, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition.

Table C-1: GENERATE AC Command Validation Error Responses

SW1 SW2	Condition
'6700'	• The length of the command data field is inconsistent with the length of data requested using the CDOL (CDOL 1 for the first GENERATE AC command, or CDOL 2 for the second GENERATE AC command). • The length of the command data field is shorter than the minimum length for the Cryptogram Version (that is, data needed to generate the Application Cryptogram has not been provided).
'6A81'	• The cryptogram requested at first GENERATE AC is not a TC, ARQC or AAC. • The cryptogram requested at second GENERATE AC is not a TC or AAC. • The P2 parameter contains a value other than '00'.

If the card receives more than two GENERATE AC commands in a transaction, then the card shall respond to the third and all subsequent GENERATE AC commands with an SW1 SW2 equal to '6985' and shall not generate a cryptogram and shall not generate a dynamic signature.

If the application is permanently blocked, it shall discontinue processing the command, shall not generate a cryptogram, shall not generate a dynamic signature, and shall respond to the GENERATE AC command with SW1 SW2 = '6985'.

Note: *A permanently blocked application should not receive any GENERATE AC commands.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 *EMV Book 3*, section 6.5.6.

C.7.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

If the P1 P2 parameters of the command have a value other than '0000', the card shall respond with an SW1 SW2 that indicates an error and should return SW1 SW2 = '6A81' (Function not supported).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.8 GET DATA Command—Response APDUs

The GET DATA command shall be performed as described in *EMV Book 3*, section 6.5.7. 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 *EMV Book 3*, is mandatory in the card for retrieval of the tagged Visa proprietary data listed in Table A-1 with “GET DATA (SD)” in the retrieval entry during non-financial processing.

The GET DATA command shall support retrieval of constructed data objects, as defined in this appendix.

Note: *The operating system is not required to support the full range of the GET DATA command as described in ISO/IEC 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 issuer-controlled devices are required to retrieve the data listed in Table A-1 with “GET DATA (SD)” in the retrieval entry to allow verification of the data during testing.

The data elements listed in Table A-1 with “GET DATA (SD)” in the retrieval entry shall be retrievable by special issuer-controlled devices using the GET DATA command if they are present on the card. Terminals do not use the GET DATA command to retrieve this data at the point of transaction.

- If the P1 P2 parameters contains the tag of a constructed data object (such as a template tag), then the GET DATA command shall return all primitive data objects contained within the constructed data object as follows:
  - The primitive data objects within the template may be returned in any order.
  - Padding bytes of '00' may occur within the template, but must be before, between, or after the primitive BER-TLV encoded data objects.
  - Padding shall not be applied within the primitive data objects.
  - Padding shall not occur outside the template.
  - The length of a padded constructed data object shall include any padding bytes present in the GET DATA response.
  - It is not possible to retrieve only part of a constructed data object.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– The data field of the response message consists of the constructed data object in BER-TLV format as illustrated (without showing optional padding) in Table C-2.

Table C-2: GET DATA Response Data Field for Constructed Data Object

Constructed Data	Constructed Data	Constructed Data Object Value			Status
Object Tag	**Object Length**	Primitive TLV_1	...	Primitive TLV_x	**Word**

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. If an issuer elects to have terminal velocity checking performed, then the issuer shall use a card that supports 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, then retrieval of the Last Online ATC Register using GET DATA is required.

C.8.3 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

- For the error conditions shown in Table C-3, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition.

Table C-3: GET DATA Command Validation Error Responses

SW1 SW2	Condition
'6A81'	The data is not allowed to be retrieved.
'6A88'	• The value of P1 P2 is not a recognized tag or template tag. • During a financial transaction, the requested data cannot be returned because it is proprietary data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.9 GET PROCESSING OPTIONS Command—Response APDUs

The GET PROCESSING OPTIONS command shall be performed as described in *EMV Book 3*, section 6.5.8.

Data retrievable by the GET PROCESSING OPTIONS command is shown in Table C-4.

Table C-4: Data Retrieval Using GET PROCESSING OPTIONS

Data Element	Tag
Application Interchange Profile	'82'
Application File Locator	'94'

The data field returned in the response to the GET PROCESSING OPTIONS command shall be coded according to either Format 1 or Format 2 as described in *EMV Book 3*, section 6.5.8.4.

C.9.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-5, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition..

Table C-5: GET PROCESSING OPTIONS Command Validation Error Responses

SW1 SW2	Condition
'6985'	• The length of the command data field is inconsistent with the length of data requested using the PDOL (that is, data needed to choose between options for processing the transaction has not been provided) • The length of the command data field is shorter than the minimum length of 2 bytes (for the '83' tag and a length byte).
'6A81'	The P1 P2 parameters contain a value other than '0000'.

If the card receives more than one GET PROCESSING OPTIONS command after the final SELECT command for the same transaction, then for the second and any subsequent GET PROCESSING OPTIONS commands the card shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If the application is permanently blocked, then the card discontinues processing the command and responds with SW1 SW2 = '6985' (Conditions of use not satisfied), which permits another application to be selected (see section).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.10 INTERNAL AUTHENTICATE Command—Response APDUs

The INTERNAL AUTHENTICATE command shall be performed as described in *EMV Book 3*, section 6.5.9.

The data field returned in the response to the INTERNAL AUTHENTICATE command shall be coded according to either Format 1 or Format 2 as described in *EMV Book 3*, section 6.5.9.4.

C.10.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-6, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition.

Table C-6: INTERNAL AUTHENTICATE Command Validation Error Responses

SW1 SW2	Condition
'6700'	The length of the command data field is inconsistent with the length personalized for the DDOL.
'6A81'	The P1 P2 parameters contain a value other than '0000'.

If the card receives more than one INTERNAL AUTHENTICATE command for a single value of the ATC, then for the second and all subsequent INTERNAL AUTHENTICATE commands the card shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied) and shall not generate the dynamic signature.

If the application is permanently blocked, then the card shall discontinue processing the command, shall not generate the dynamic signature, and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.11 PIN CHANGE/UNBLOCK Command—Response APDUs

The PIN CHANGE/UNBLOCK command is a post-issuance command to unblock the reference PIN (allowing more PIN tries) or to simultaneously change and unblock the reference PIN.

The PIN CHANGE/UNBLOCK command shall be performed as described in *EMV Book 3*, section 6.5.10.

The command data field shall contain the PIN data if the PIN is changing and the 4 or 8 byte MAC generated using the Format 2 method described in *EMV 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. 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.)
- **'02'**—PIN CHANGE/UNBLOCK with PIN data generated without using current PIN (See section C.11.2.)

C.11.1 PIN Data Generated Using the Current PIN

If the P2 parameter in the command is equal to '01', then the PIN data is generated as follows:

1. The issuer determines the issuer's unique Master Derivation Key (MDK) used to generate the card application's Unique DEA Key A and B (UDK-A and UDK-B) and the Data Encipherment Master Derivation Key A and B (ENC MDK-A and ENC MDK-B) used to generate the card application's Data Encipherment Unique DEA key (ENC UDK). Both keys are used in this operation.
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. ENC UDK A and B are used to derive the Data Encipherment Session Keys.
4. The issuer determines the new Reference PIN for the card's application and the length of the new PIN.

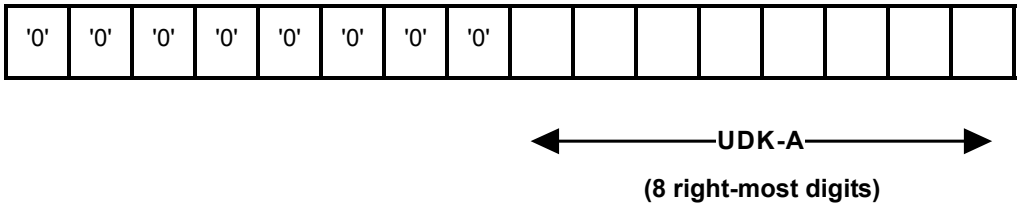
Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

5. Using the UDK-A, the issuer creates a 16-hexadecimal digit PIN block as follows:

   a. Create a 16-hexadecimal digit block of data by extracting the eight rightmost digits of the card application's Unique DEA Key A (UDK-A) and zero-filling it on the left with '00 00 00 00', as shown in Figure C-1:

Note: *DES keys are by definition (FIPS 46-3) of odd parity. The UDK-A bits used in Figure C-1 include any adjustments made for parity of the UDK-A.*

Figure C-1: Input Block based on UDK-A



   b. Create the second 16-hexadecimal digit block of data (see Figure C-2) by taking the new PIN and adding a pad character of '0' 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 'F's.

Figure C-2: Input Block based on New PIN

'0'	N	P	P	P	P	P/'F'	P/'F'	P/'F'	P/'F'	P/'F'	P/'F'	P/'F'	P/'F'	'F'	'F'

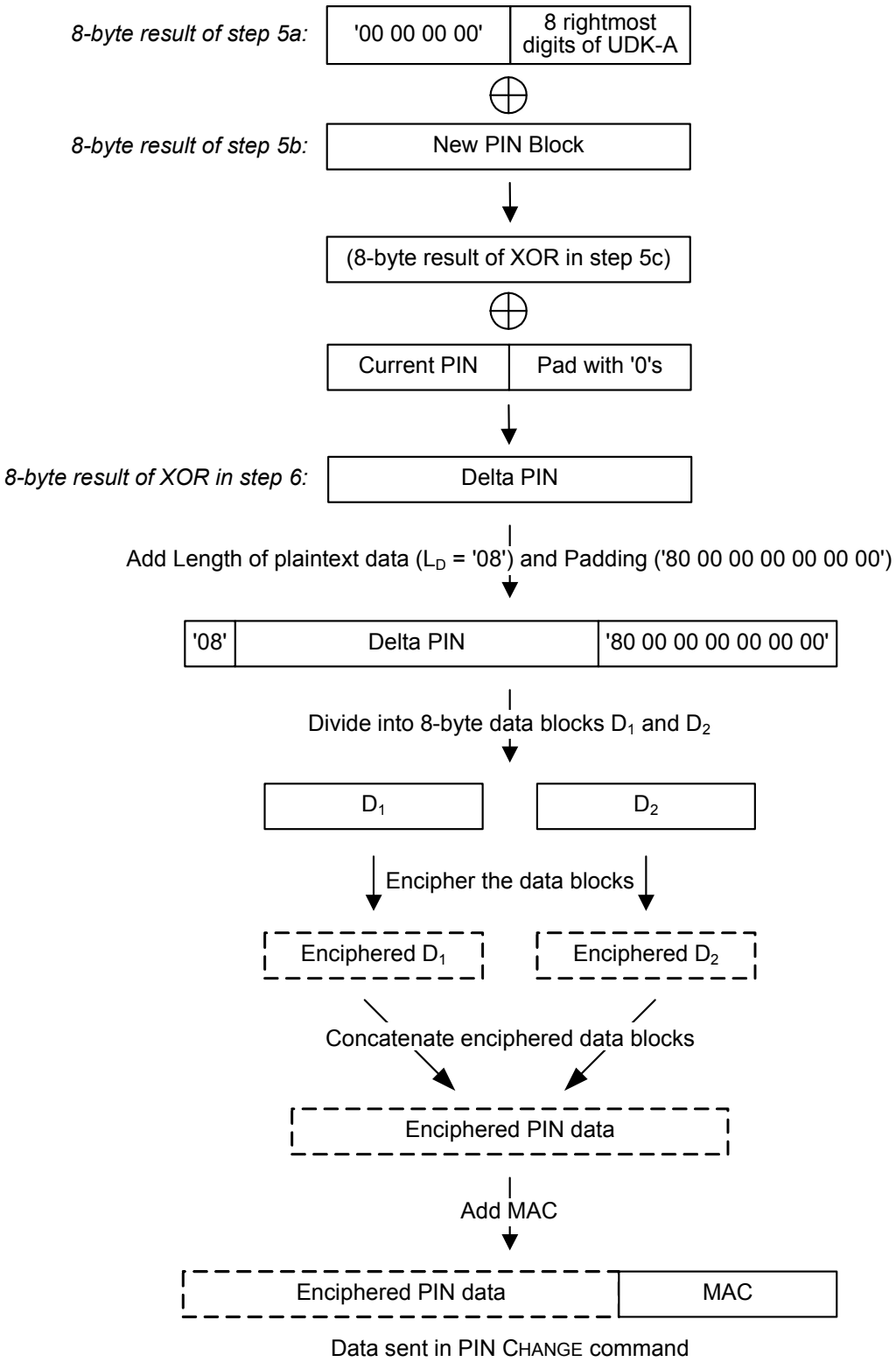
   c. Perform an exclusive-OR operation on these two blocks of data.

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 '0's. 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure C-3: Generation of PIN CHANGE Command Data With Current PIN



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.11.2 PIN Data Generated Without Using the Current PIN

If the P2 parameter in the command is equal to '02', then the PIN data is generated using either of the follow PIN Block formats:

- VIS Legacy PIN Block Format: The special Visa PIN Block format that was defined in the previous versions of VIS. This method can be used only in combination with CVN 10 and CVN 18.
- ISO PIN Block Format: A format introduced in VIS version 1.6, that is using standard ISO 9594-1 PIN Block formats. This method can be used only in combination with CVN '22'.

In the following sections, the two formats are defined.

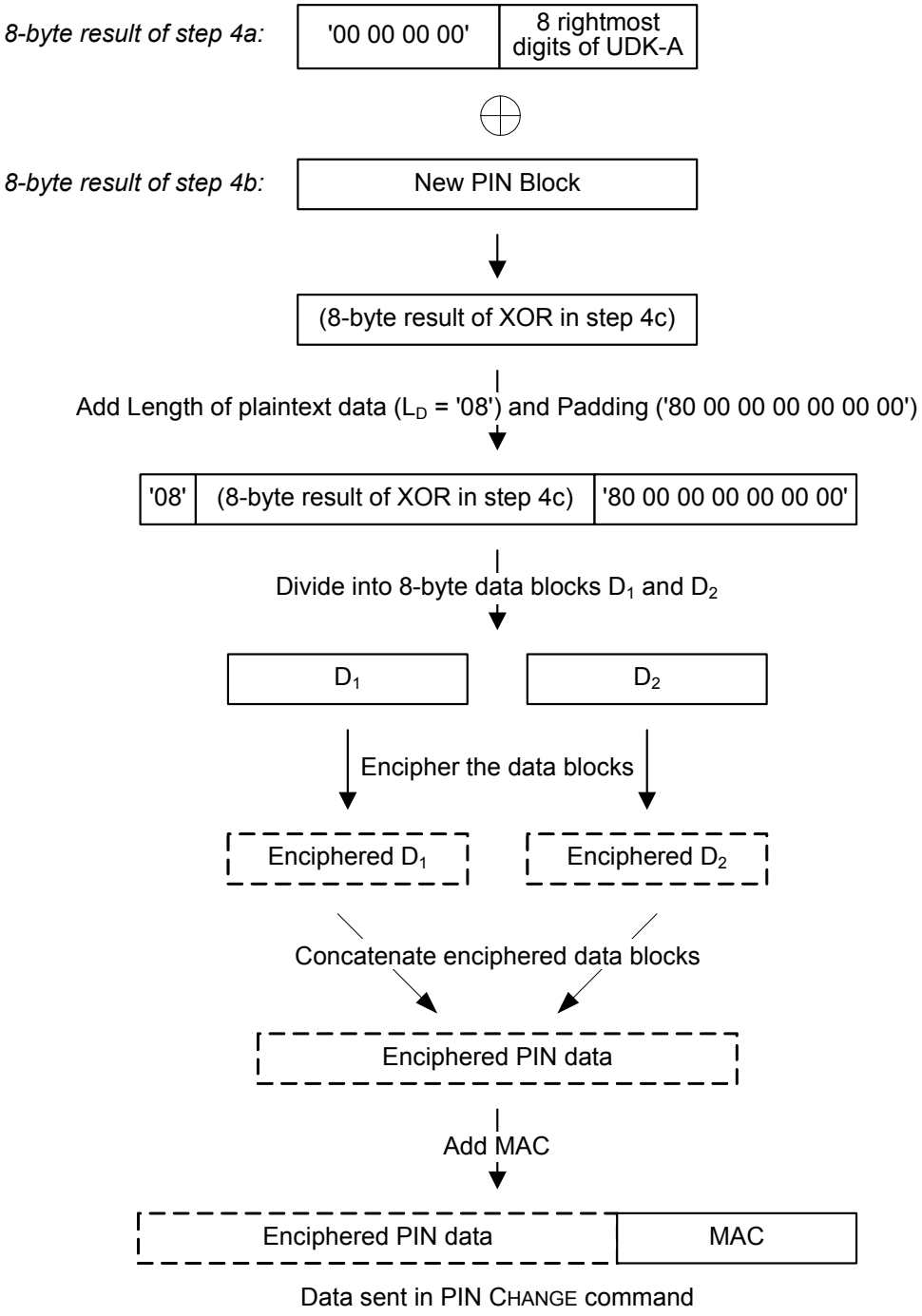
C.11.2.1 VIS Legacy PIN Block Format Generated Without Using the Current PIN

The PIN Block format is built by performing the following steps:

1. The issuer determines the issuer's unique Master Derivation Key (MDK) used to generate the card application's Unique DEA Key A and B (UDK-A and UDK-B) and the Data Encipherment Master Derivation Key A and B (ENC MDK-A and ENC MDK-B) used to generate the card application's Data Encipherment Unique DEA key (ENC UDK). Both keys are used in this operation.
2. The issuer generates the Data Encipherment Session Keys, as described in Appendix B, Secure Messaging. ENC UDK A and B are used to derive the Data Encipherment Session Keys.
3. The issuer determines the new Reference PIN for the card's application and the length of the new PIN.
4. Using the UDK-A, 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 Unique DEA Key A (UDK-A) and zero-filling it on the left with '00 00 00 00', as shown in Figure C-1.
   b. Create the second 16-hexadecimal digit block of data (see Figure C-2) by taking the new PIN and adding a pad character of a '0' 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 'F's.
   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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure C-4: Generation of PIN CHANGE Command Data Without Current PIN



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.11.2.2 ISO PIN Block Format Generated Without Using the Current PIN

The PIN Block format is built by performing the following steps:

1. The issuer determines the issuer's unique Data Encipherment Master Derivation Key A and B (ENC MDK-A and ENC MDK-B) 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 section B.4.2, EMV Common Session Key Generation. ENC UDK A and B are used to derive the Data Encipherment Session Keys.
3. The issuer determines the new Reference PIN for the card's application and the length of the new PIN.
4. The issuer creates the 16-hexadecimal PIN Block by taking the new PIN and adding a control character of C 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 filler or transaction digits, as shown in Figure C-5 or C-6.

Note: *Issuers are cautioned to ensure their Issuer Script commands use a PIN Block Format that is supported by their chosen card products.*

Figure C-5: ISO PIN Block Format 1

C	N	P	P	P	P	P/T	P/T	P/T	P/T	P/T	P/T	P/T	P/T	F	F

Where:

	Name	Value
C	Control Field	'1'
N	PIN Length	'4' to 'C'
P	PIN Digit	'0' to '9'
P/F	PIN/Transaction Digit	Determined by PIN Length
T	Transaction Digit	'0' to 'F'

Note: *This is the PIN Block defined in ISO 9564-1 as Format 1 PIN Block.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure C-6: ISO PIN Block Format 2

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

Where:

	Name	Value
C	Control Field	'2'
N	PIN Length	'4' to 'C'
P	PIN Digit	'0' to '9'
P/F	PIN/Filler	Determined by PIN Length
F	Filler	'F'

Note: *This is the PIN Block defined in ISO 9564-1 as PIN Block Format 2, and is the same PIN Block defined in EMV, book 3 for the VERIFY command.*

5. The issuer enciphers the PIN block created in Step 4 with the Data Encipherment Session Keys to generate the PIN data.

C.11.3 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-7, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition..

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table C-7: PIN CHANGE/UNBLOCK Command Validation Error Responses

SW1 SW2	Condition
'6700'	For PIN CHANGE, the length of the command data is not a valid length for the expected PIN block plus MAC
'6988'	For PIN CHANGE, the PIN block format is not valid
'6A81'	• The P1 parameter of the PIN CHANGE/UNBLOCK command does not have the value '00' • The P2 parameter of the PIN CHANGE/UNBLOCK command contains a value not supported by the command

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.12 PUT DATA Command—Response APDUs

The PUT DATA command is a post-issuance command that updates specific primitive and constructed data objects stored in the card. A data object can be updated with this command only if it has a tag associated with it.

Section A.1 indicates those data elements that may be updated using the PUT DATA command. If the Issuer Update entry in Table A-1 for a data element indicates that no update is allowed (either a “N” or a “n/a”), then updates to the data element using PUT DATA shall not be allowed unless it is part of a larger data element that is allowed to be updated; in which case, the value after update of the larger data element shall be the same as the value before the update. The application does not enforce this requirement, it is a requirement on the issuer script command sent to the application. For example, the Issuer Application Data may be updated by a PUT DATA command, but the value of the CVR after the update shall be the same as the value before the update.

All data elements listed with PUT DATA in the Issuer Update entry in Table A-1 shall be supported for PUT DATA if the PUT DATA issuer script command is supported and the data element is present in the application.

C.12.1 Command Message

The PUT DATA command message is coded according to Table C-8.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table C-8: PUT DATA Command Message

Code	Value
CLA	'04'
INS	'DA'
P1 P2	If P1 P2 has the value '0000', the data field contains one or more primitive data objects (in BER-TLV format) to be updated. All other values indicate the tag of the primitive data object or template tag of the constructed data object to be updated.
Lc	Length of command data field
Data	If P1 P2 contains the tag for a primitive data object, contains: • the new value for a primitive data object • followed by a 4 or 8 byte MAC. The MAC value is not preceded by a tag and length. If P1 P2 has the value '0000', contains: • one or more primitive data objects to be updated, each in BER-TLV format. • followed by a 4 or 8 byte MAC. The MAC value is not preceded by a tag or length. If P1 P2 contains the template tag for a constructed data object, contains • one or more primitive data elements, each in BER-TLV- format and identified by a tag understood within the context of the template. • followed by a 4 or 8 byte MAC. The MAC value is not preceded by a tag or length.
Le	Not present

The MAC contained in the data field is generated using Format 2. The MAC is generated as described in Appendix B, Secure Messaging.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The PUT DATA command message is coded according to Table C-9 or Table C-10.

Table C-9: PUT DATA Command Data for P1 P2 = Primitive Data Element Tag

Primitive Data element Value	MAC Value
Value	V_{MAC}

Table C-10: PUT DATA Command Data for P1 P2 = '0000' or Template Tag

First Data Element in BER-TLV Format				Final Data Element in BER-TLV Format			MAC Value
T_1	L_1	V_1	...	T_x	L_x	V_x	V_{MAC}

Updates to constructed data objects contain a template tag in P1 P2. The data field is BER-TLV coded (with the tags having meaning specific to that template), and may contain any combination of the following:

- if the primitive data element identified by a tag in the template is already present in the template, then the new value is a complete replacement for the existing value, possibly with a different length. Partial update of a single data element within the template is not supported.
- if the primitive data element identified by a tag in the template is not already present in the template; then the tag, length and value defines an additional primitive data element to be added to the template (if the application has sufficient room remaining in the template).

Note: *Data elements may be personalized with padding bytes of '00' before, between, and after the primitive data elements within a template to reserve room for future updates.*

Primitive data elements already present in the template that are not included in the command data are not changed.

When multiple primitive data objects are to be updated with a single PUT DATA command (using either a template tag for a constructed data element, or P1 P2 = '0000'), implementations shall ensure that either all of the data objects are updated if the command is successful, or none of the data objects are updated if the command fails.

Note: *If a PUT DATA issuer script command received before the second GENERATE AC command updates any data elements that are used during processing of the second GENERATE AC command, then the updated value(s) shall be used during processing of the second GENERATE AC command.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.12.2 Reset Offline Funds with Update to Funds Limits

Instead of automatically resetting CTTA (to zero) and VLP Available Funds (to the VLP Funds Limit) automatically during Completion Processing, the issuer might prefer to only reset them using the PUT DATA issuer script command, and uses options in the ADA to control this special behavior as follows:

- The card resets the Cumulative Total Transaction Amount (CTTA) to zero if *both* of the following are true:
  - PUT DATA to Cumulative Total Transaction Amount Limit (CTTAL) is successful
  - The ‘Do not reset CTTA during GENERATE AC’ bit of the ADA is set to 1b
- The card resets VLP Available Funds to the VLP Funds Limit if *all* of the following are true:
  - The PUT DATA to VLP Funds Limit is successful
  - The ‘Do not reset VLP Available Funds during GENERATE AC’ bit of the ADA is set to 1b

C.12.3 Update AIP and AFL

If Profiles Functionality is not supported, and update to the AIP and AFL used for contact transactions is supported, then a PUT DATA to 'DF11' in 'BF5A' (the AIP/AFL template) shall update the AIP and AFL that are sent in the GET PROCESSING OPTIONS response for contact transactions.

C.12.4 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-11, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition.

Table C-11: PUT DATA Command Validation Error Responses

SW1 SW2	Condition
'6700'	The length of the updated data element (after applying the updates in the PUT DATA command) would be longer than the space available for the data element (for example, longer than the space reserved for the data element at the time of perso)
'6A88'	The P1 P2 parameters contain a value other than '0000' that is not a recognized tag (or template tag).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The warning and error conditions shown in Table C-12 may be returned by the card.

Table C-12: PUT DATA Command Message Error Conditions

SW1 SW2	Meaning	Type
'6200'	No information given	Warning
'6281'	Data may be corrupted	Warning
'6400'	No precise diagnosis	Error
'6581'	Memory failure	Error
'6700'	Wrong length (Lc)	Error
'6882'	Secure messaging not supported	Error
'6982'	Security status not supported	Error
'6986'	Command not allowed	Error
'6987'	Secure messaging data object missing	Error
'6988'	Secure messaging data object incorrect	Error
'6A80'	Incorrect parameter in data field	Error
'6A81'	Function not supported	Error
'6A84'	Not enough memory space in file	Error
'6A85'	Lc inconsistent with TLV structure	Error
'6A88'	Referenced data not found	Error

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.13 READ RECORD Command—Response APDUs

The READ RECORD command shall be performed as described in *EMV Book 1*, section 11.2, and *EMV Book 3*, section 6.5.11.

All records listed in any of the AFLs for contact shall be retrievable over the contact interface. This record retrieval restriction applies regardless of whether or not the AFL was returned by the card prior to the card application receiving the READ RECORD command.

C.13.1 Processing the Profile Selection File Entries

If Profiles Functionality is supported:

- special issuer-controlled devices shall use the Profile Selection File Entry data element to determine the location (SFI) and number of records to read in the Profile Selection File.
- The application shall support retrieval using the READ RECORD command of the Profile Selection Entries listed in the Profile Selection File Entry.

C.13.2 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-13, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition.

Table C-13: READ RECORD Command Validation Error Responses

SW1 SW2	Condition
'6A81'	Bits 3-1 of the P2 parameter of the READ RECORD command do not have the value 100b.
'6A82'	Bits 8-4 of the P2 parameter of the READ RECORD command do not indicate a recognized SFI in the range 1–30 ('01' – '1E').
'6A83'	• The record requested by the READ RECORD command is not a recognized record in the SFI. • The record requested by the READ RECORD command is not allowed to be retrieved over the interface (for example, a record only listed in an AFL used for the contactless interface is not allowed to be retrieved over the contact interface, or the Transaction Log may be personalized to not allow it to be retrieved over the interface used for the transaction).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.14 SELECT Command—Response APDUs

The SELECT command shall be performed as described in *EMV Book 1*, section 11.3.

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 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)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.15 UPDATE RECORD Command—Response APDUs

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

UPDATE RECORD command processing does not enforce the requirement in Table A-1 to not update a specific data element in a record. Instead, this is a requirement on the UPDATE RECORD issuer script command sent to the application. For example, the record that contains the Application Expiration Date may be updated, but the value of the Application Expiration Date after the update shall be the same as the value before the update.

C.15.1 Command Message

The UPDATE RECORD command message is coded according to the values in Table C-14.

Table C-14: 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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

P2 is structured as shown in Table C-15.

Table C-15: UPDATE RECORD Reference Control Parameter

Bits	Value	Meaning
b8-b4	xxxxx (where xxxxx is a binary value from 1 to 30)	SFI
b3-b1	100b	Record number is in P1

The command data field consists of the new record contents followed by a 4 or 8 byte MAC generated using Format 2. The MAC is generated as described in Appendix B, Secure Messaging.

The new record contents sent in the command data field shall be a complete replacement for the existing record (including the record template tag '70' if the record requires the template tag). Partial update of a record is not supported.

Note: *Profile Selection Entries do not contain the template tag '70' because the Profile Selection File is not in an SFI in the range from 1 to 10.*

C.15.2 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-16, the card shall respond with an SW1 SW2 that indicates an error and should return the recommended error condition.

Table C-16: UPDATE RECORD Command Validation Error Conditions

SW1 SW2	Condition
'6A81'	Bits 8-4 of the P2 parameter of the UPDATE RECORD command indicates an SFI that is not updateable (for example, the SFI of the Transaction Log)
'6A82'	Bits 8-4 of the P2 parameter of the UPDATE RECORD command do not indicate a recognized SFI in the the range 1–30 ('01' – '1E')
'6A83'	The record indicated for the UPDATE RECORD command is not a recognized record in the SFI
'6A86'	Bits 3-1 of the P2 parameter of the UPDATE RECORD command do not have the value 100b

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The warning and error conditions shown in Table C-17 may be returned by the card.

Table C-17: UPDATE RECORD Response Additional Error and Warning Conditions

SW1 SW2	Meaning	Type
'6200'	No information given	Warning
'6281'	Data may be corrupted	Warning
'6400'	No precise diagnosis	Error
'6581'	Memory failure	Error
'6700'	Wrong length (Lc)	Error
'6882'	Secure messaging not supported	Error
'6981'	Command incompatible with file organization	Error
'6982'	Security status not satisfied	Error
'6986'	Command not allowed	Error
'6987'	Secure messaging data object missing	Error
'6988'	Secure messaging data object incorrect	Error
'6A81'	Function not supported	Error
'6A82'	File not found	Error
'6A83'	Record not found	Error
'6A84'	Not enough memory space in file	Error
'6A85'	Lc inconsistent with TLV structure	Error
'6A86'	Incorrect parameters P1 P2	Error

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

C.16 VERIFY Command—Response APDUs

The VERIFY command shall be performed as described in *EMV Book 3*, section 6.5.12.

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.

C.16.1 Processing State Returned in the Response Message

A successful execution of the command is coded by SW1 SW2 = '9000'.

For the error conditions shown in Table C-18, the card shall not decrypt the PIN block, shall respond with an SW1 SW2 that indicates an error, and should return the recommended error condition.

Table C-18: VERIFY Command Validation Error Responses

SW1 SW2	Condition
'63Cx'	PIN verification failed. The value of “x” indicates the value of the PIN Try Counter (i.e., the number of PIN tries remaining).
'6984'	• The P1 parameter contains a value other than '00'. • The P2 parameter contains a value not supported by the command. • The length of the command data field is not a valid length for the expected PIN block. • The PIN block format is not valid.

If the application is permanently blocked, then the card shall discontinue processing the command, shall not verify the PIN, and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D Authentication Data, Keys and Algorithms

This appendix describes the keys and algorithms associated with the generation of the Application Cryptograms – Application Authentication Cryptogram (AAC), Transaction Certificate (TC), and Authorization Request Cryptogram (ARQC) – and the Authentication Response Cryptogram (ARPC).

This appendix includes the following sections:

D.1 Source Data for Application Cryptograms (TC, AAC, ARQC)
D.2 Application Cryptograms
D.3 CVN 10 (Cryptogram Version Number = '0A')
D.4 CVN 18 (Cryptogram Version Number '12') and CVN '22'
D.5 CVN 12 ('0C'), CVN '2C', and CVN 50 ('32') - CVN 59 ('3B')
D.6 Data Conversion
D.7 Derivation Key Methodology
D.8 Host Security Modules (HSM)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.1 Source Data for Application Cryptograms (TC, AAC, ARQC)

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 VIS, the methods for generating the TC, AAC and the ARQC types of Application Cryptogram are identical for a given Cryptogram Version Number.)

A data object to be input to the TC, AAC or ARQC algorithm is obtained by the card from one of the 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.
- 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 VIS, issuer proprietary data shall not be input to the cryptograms.
- The cryptogram versions defined in this version of VIS do not use a TDOL. For proprietary cryptograms, 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. See EMV Book 3, section 9.2.2 for information on use of the TDOL and TC Hash Value.

  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.*

Visa supports a limited set of methods to create Application Cryptograms (a TC, AAC, and ARQC). Each method is identified by a Cryptogram Version Number. See section D.2 for detailed information on the Visa-supported cryptogram methods and section D.2.1for information on the valid CVN values.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The Cryptogram Version Number indicates:

- The set of data used to generate the application cryptogram
- Elements from the terminal that are to be hashed (if any) before being sent to the card for generation of the application cryptogram
- The method used to generate a session key, if used
- The method of padding the data elements prior to generating the cryptogram
- The format of the Issuer Application Data being sent in the authorization request
- The method to be used for generating the Authorization Response Cryptogram (ARPC) if one is sent in the authorization response
- The format to be used for the Issuer Authentication Data if it is sent in the authorization response.

In this version of VIS, the source of the data objects is identical for the TC, AAC, and ARQC algorithms.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.2 Application Cryptograms

D.2.1 Cryptogram Version Numbers (CVNs) Supported

The method used to create a Transaction Certificate (TC), Application Authentication Cryptogram (AAC), or Authorization Request Cryptogram (ARQC) type Application Cryptogram is identified by a CVN. Visa currently supports the following CVNs and defines two methods for generating an Application Cryptogram, with each described further in following sections:

- CVN 10 ('0A') – defined by this specification
- CVN 18 ('12') – defined by this specification
- CVN 12 ('0C'), CVN '2C', and CVN 50 ('32') through CVN 59 ('3B') – defined by the issuer
- CVN '22' – defined by this specification

D.2.2 Application Cryptogram Algorithm

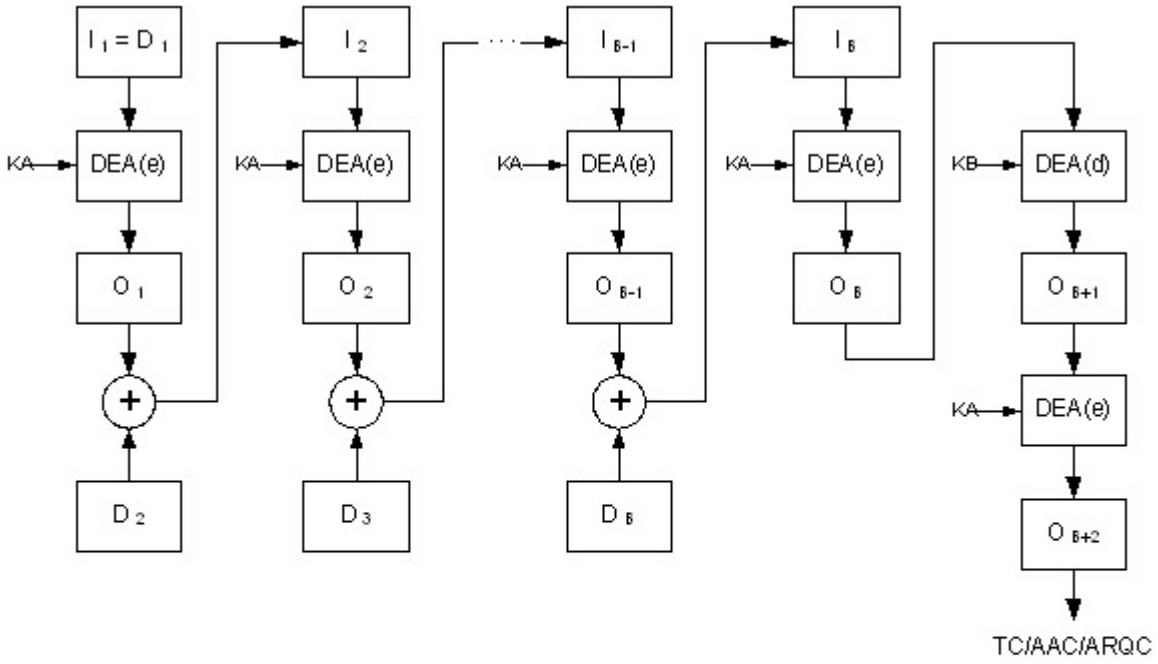
This section shows the algorithm to generate the Application Cryptogram (TC, AAC or ARQC) for CVN 10, 18 and '22', as shown in Figure D-1.

For CVN 10, Key A and Key B refer to Unique DEA Key A and B.

For CVN 18 and '22', Key A and Key B refer to Session Key A and B described in section D.7.2.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure D-1: Algorithm for Generating the Application Cryptogram (TC, AAC or ARQC)



Legend

I =	Input	D =	Data block
DEA(e) =	Data Encryption Algorithm (encipherment mode)	KA =	Key A
		KB =	Key B
DEA(d) =	Data Encryption Algorithm (decipherment mode)	⊕ =	Exclusive-OR
O =	Output		

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.3 CVN 10 (Cryptogram Version Number = '0A')

D.3.1 Data Input for CVN 10 ('0A')

The data input to generation of a TC, AAC, or ARQC Application Cryptogram using CVN 10 is described in Table D-1 and illustrates:

- The set of data used to generate the cryptogram (Table D-1 lists the eleven mandatory data elements required for CVN 10)
  - 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
- The order in which the data is to be input to the cryptographic algorithm
- Terminal hashing is not supported for CVN 10

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table D-1: Data Input for TC, AAC and ARQC With CVN 10 ('0A')

Data Element	Plaintext Data from Terminal (requested in CDOL1 and CDOL 2)	Input by Card
Amount, Authorized	X	
Amount, Other	X	
Terminal Country Code	X	
Terminal Verification Results (TVR)	X	
Transaction Currency Code	X	
Transaction Date	X	
Transaction Type	X	
Unpredictable Number	X	
Application Interchange Profile		X
ATC		X
Card Verification Results		X

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. Details can be found in the current version of the *VSDC System Technical Manual*.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.3.2 Generating the Application Cryptogram (TC, AAC, and ARQC) for CVN 10 ('0A')

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, then 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.

   For CVN 10, the remaining right-most bits in the last data block shall be zero filled.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

4. Using triple DEA encipherment, the card shall perform the algorithm shown in Figure D-1 of section D.2.2 to generate the TC, AAC or ARQC using the Unique DEA Keys A and B for CVN 10.

   Note: *For CVN 10, Key A and Key B refer to Unique DEA Key A and B.*

   If Issuer Script failed, then the terminal sets the 'Issuer Script processing failed after final GENERATE AC command' bit of the Terminal Verification Results to 1b after the TC or AAC is generated by the card. Therefore, prior to validating the TC or AAC transmitted in the clearing message, this bit needs to be reset to 0b. Otherwise, the TC or AAC cannot be correctly validated.

   The algorithm used in step 4 with five data blocks, D1, D2, D3, D4 and D5 is identical to the algorithm described in VIS 1.5.

D.3.3 Generating the Authorization Response Cryptogram (ARPC) for CVN 10 ('0A')

The Authorization Response Cryptogram (ARPC) for CVN 10 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 ⊕ ARPC 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 ARPC 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 ARPC Response Code in an 8-byte field and zero fills ('0') the remaining 6 bytes. (As discussed in section D.6, the ARPC 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).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 Number 10. 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.

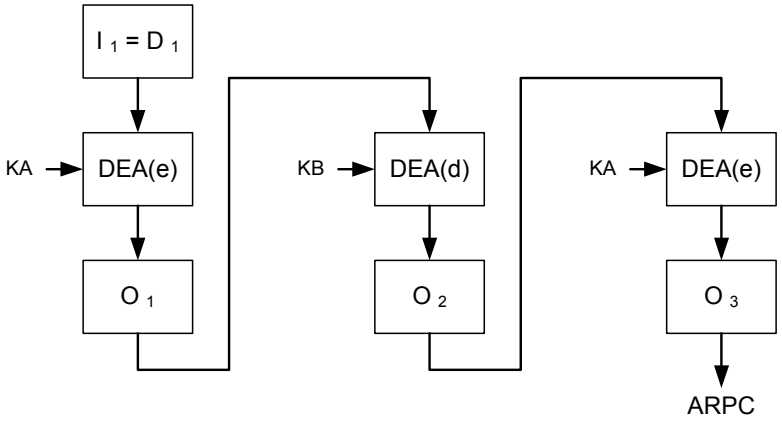
   Note: *For Cryptogram Version Number 10, Key A and Key B refer to Unique DEA Key A and B.*

D.3.4 Format of Issuer Authentication Data (IAuD) for CVN 10 ('0A')

The Issuer Authentication Data (IAuD) for CVN 10 consists of the following data:

- Authorization Response Cryptogram (ARPC) - 8 bytes
- ARPC Response Code - 2 bytes

Figure D-2: Algorithm for Generating the ARPC for CVN 10



Legend:

I =	Input	D =	Data block
DEA(e) =	Data Encryption Algorithm (encipherment mode)	KA =	Key A
		KB =	Key B
DEA(d) =	Data Encryption Algorithm (decipherment mode)		
O =	Output		

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.4 CVN 18 (Cryptogram Version Number '12') and CVN '22'

All products shall be capable of supporting CVN 18, and may optionally support additional CVNs, including CVN '22' and proprietary CVNs. It is the issuer's choice which CVN to use for their cards.

D.4.1 Data Input for CVN 18 ('12') and CVN '22'

The data input to generation of a TC, AAC, or ARQC Application Cryptogram using CVN 18 or CVN '22' is described in Table D-2, and illustrates:

- The set of data used to generate the cryptogram
  - 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
- The order in which the data is to be input to the cryptographic algorithm
- Terminal hashing is not supported for CVN 18 or CVN '22'

Note: *The algorithm for generating the Application Cryptogram for CVN 18 and CVN '22' is described in section D.4.2 and is the same as that described in the CCD Part of EMV Book 2, section 8.1.2 for an application with a cryptogram defined by the Common Core Definitions with a Cryptogram Version of '5'.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table D-2: Data Input for TC, AAC, ARQC With CVN 18

Data Element	Plaintext Data from Terminal (requested in CDOL1 and CDOL 2)	Input by Card
Amount, Authorized	X	
Amount, Other	X	
Terminal Country Code	X	
Terminal Verification Results (TVR)	X	
Transaction Currency Code	X	
Transaction Date	X	
Transaction Type	X	
Unpredictable Number	X	
Application Interchange Profile		X
ATC		X
Issuer Application Data		X

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. Details can be found in the current version of the *VSDC System Technical Manual*.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.4.2 Generating the Application Cryptogram (TC/AAC/ARQC) for CVN 18 ('12') and CVN '22'

The TC, AAC, and ARQC are generated by putting selected data (see section D.4.1) into the algorithm described in the CCD Part of EMV Book 2, section 8.1.2, for an application with a cryptogram defined by the Common Core Definitions with a Cryptogram Version of '5'. This process includes four steps, summarised as follows:

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.

   The TC Hash Value is not referenced in CDOL1 for CVN 18.

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 data listed in Table D-2 in the order specified to create a block of data:

3. The card shall format this block of data into 8-byte data blocks, labeled D1, D2, D3, D4, and so on.

   The data shall be padded with a mandatory '80' byte and the remaining right-most bits in the last data block are zero filled.

4. The card shall generate AC Session Key A and AC Session Key B as described in section D.7.2

   The card shall generate the 8-byte Application Cryptogram using the AC session keys from step 4 to perform the MAC algorithm shown in section D.2.2.

   Note: *If Issuer Script failed after the second GENERATE AC command is processed, then the terminal sets the 'Issuer Script processing failed after final GENERATE AC command' bit of the Terminal Verification Results to 1b after the TC or AAC is generated by the card. Therefore, prior to validating the TC or AAC transmitted in the clearing message, this bit needs to be reset to 0b. Otherwise, the TC or AAC cannot be correctly validated.*

   The process to generate the Application Cryptogram for CVN 18 described in this section is identical to the process described in VIS 1.5.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.4.3 Generating the Authorization Response Cryptogram (ARPC) for CVN 18 ('12') and CVN '22'

The Authorization Response Cryptogram (ARPC) for CVN 18 and CVN '22' is generated by inputting selected data into the algorithm described in this section.

The card generates a reference ARPC for comparison to the ARPC received in the second GENERATE AC command. The generation process for the reference ARPC requires four steps:

1. The card shall concatenate the ARQC, the CSU and, if the 'Proprietary Authentication Data Included' bit of the CSU is set to 1b the Proprietary Authentication Data, to create a block of data:
   - ARQC || CSU, if the 'Proprietary Authentication Data Included' bit of the CSU is set to 0b
   - ARQC || CSU || Proprietary Authentication Data, if the 'Proprietary Authentication Data Included' bit of the CSU is set to 1b

   The ARQC transmitted in the request message is used as input to the concatenation. There is no need for the ICC to recalculate the ARQC.
2. The card formats this block of data into 8-byte data blocks, labeled D1, D2, D3 and so on.

   The data is padded with a mandatory '80' byte and the remaining right-most bits in the last data block are zero filled.
3. Generate a MAC over the block of data by applying the algorithm specified in section D.2.2 using the Application Cryptogram Session Key derived when computing the ARQC.
4. The ARPC is equal to the 4 left-most bytes of the MAC.

D.4.4 Format of Issuer Authentication Data (IAuD) for CVN 18 ('12') and CVN '22'

The Issuer Authentication Data (IAuD) for CVN 18 consists of the following data:

- Authorization Response Cryptogram (ARPC) - 4 bytes
- Card Status Updates (CSU) - 4 bytes
- (optional) Proprietary Authentication Data - 1 to 8 bytes

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.5 CVN 12 ('0C'), CVN '2C', and CVN 50 ('32') - CVN 59 ('3B')

CVN 12 ('0C'), CVN '2C' and CVN 50 ('32') through 59 ('3B') have been made available to designate issuer proprietary cryptogram processing. They may be used by issuers that do not wish to implement the key management or issuer host authentication processing associated with CVN 10 ('0A'), CVN 18 ('12') or CVN '22' in the early stages of migration, or by issuers that want to support an issuer-proprietary cryptogram.

CVN 12 and CVN 50 through CVN 59 are supported for IAD Format 0/1/3. CVN '2C' is supported only for IAD Format 2.

CDOL1 and CDOL2 shall be present in the card. The card shall respond to the GENERATE APPLICATION CRYPTOGRAM (AC) command from the terminal in compliance with the EMV specifications and bulletins.

The Derivation Key Index (DKI) can be defaulted to '00' (or any valid value) at the time of personalization if the issuer does not intend to implement key management or issuer host authentication processing immediately, or if the issuer-proprietary cryptogram does not use the DKI.

Note: *A DKI value of '00' does notalways indicate that the issuer is not implementing key management or issuer host authentication processing.*

Any cryptogram versions unknown to VisaNet will result in indication that online Card Authentication has failed.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.6 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.

EMV Book 1 and *EMV 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.6.1 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.6.2 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 '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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.6.3 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 '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 '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.6.4 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 '00' to '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.6.5 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: *For CVN 10, the ARPC 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.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

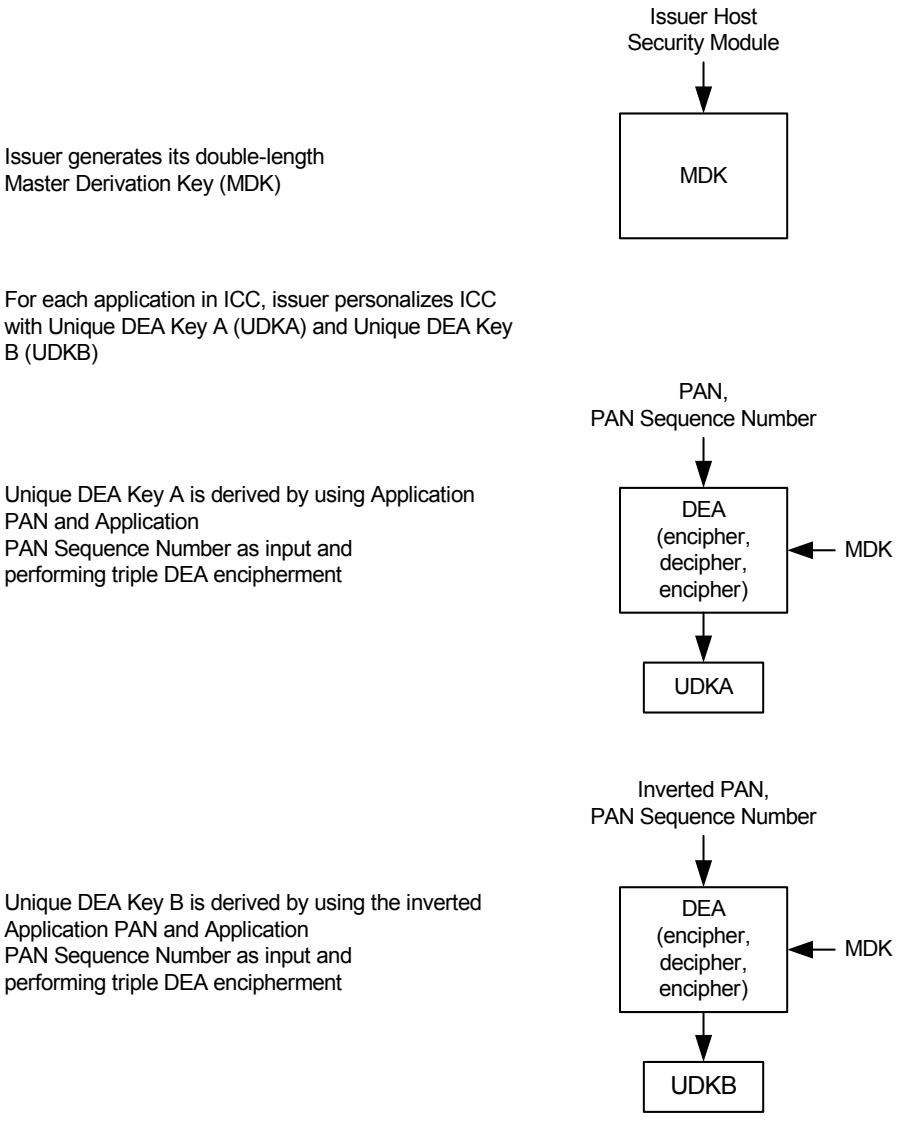
D.7 Derivation Key Methodology

D.7.1 Unique DEA Keys Derivation

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) for CVN 10, 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



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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, then 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, then the following formatting rules shall be applied:

- If the Application PAN plus the Application PAN Sequence Number are less than 16 digits, then 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, then 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 1b is set to 0b and each bit with value 0b is set to 1b.

A PAN with an uneven number of digits is padded on the left with a zero. An 'F' is not included in the concatenation of the PAN and PAN Sequence Number.

EXAMPLE:

The 19 digit PAN stored on the card is '4000001234567890123F' and the PAN Sequence Number is '01'. The concatenation result is '01 23 45 67 89 01 23 01'.

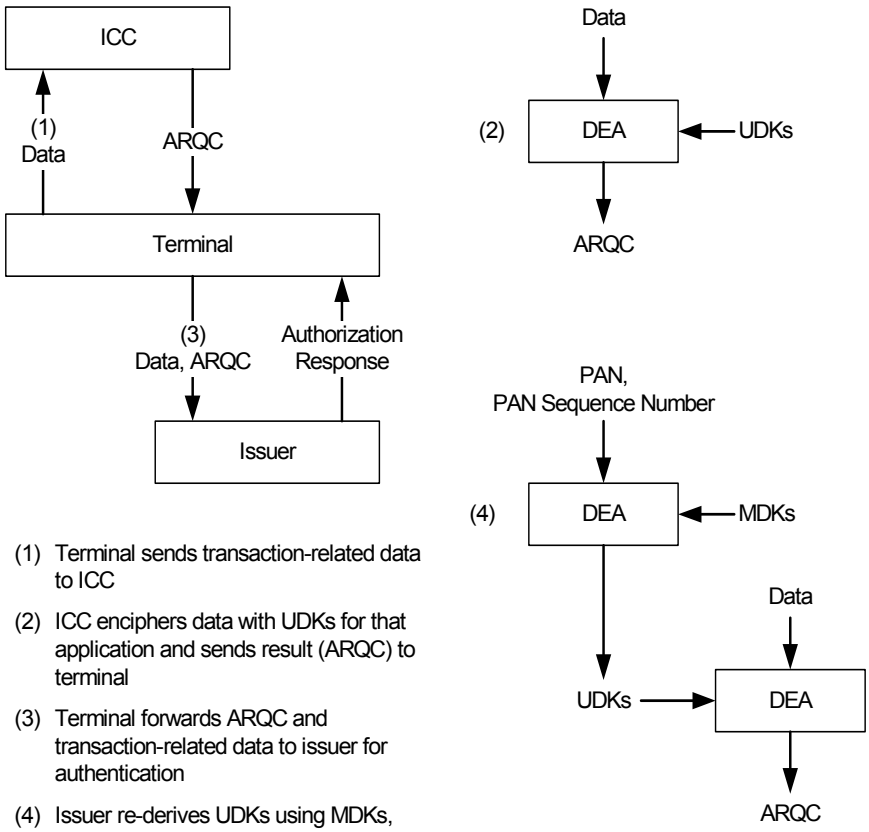
Note: *When triple DEA encipherment is performed using the issuer's double-length Master Derivation Key, the encipherment function shall always be performed using the first half of the issuer's double-length key and the decipherment function shall always be performed using the second half of the issuer's double-length key. This convention shall apply regardless of whether the Unique DEA Key A or B is being generated.*

Note: *What VIS calls the Master Derivation Key that is used to derive the UDK, in EMV is called the Issuer Master Key, IMK.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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



(1) Terminal sends transaction-related data to ICC

(2) ICC enciphers data with UDKs for that application and sends result (ARQC) to terminal

(3) Terminal forwards ARQC and transaction-related data to issuer for authentication

(4) Issuer re-derives UDKs using MDKs, Application PAN, and Application PAN Sequence Number, then verifies transmitted ARQC

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.7.2 EMV Common Session Key Derivation

The following session key derivation is identical to the method defined in EMV, Book 2, Annex A1.3.1.

This method shall be used for the Application Cryptogram generation for CVN 18 ('12') and CVN '22', and for secure messaging when performed in combination with CVN '22'.

For the session key used to generate and verify the Application Cryptogram and the ARPC for CVN 18 and CVN '22', follow the steps below:

1. The Unique DEA Keys A and B (UDK) are selected as the key K for the cryptographic process.
2. The ATC followed by 6 bytes of ‘00’ is copied to a 8-byte field to generate R:

   R := ATC || '00' || '00' || ‘00’ || '00' || '00' || '00'.

For the session key for secure messaging, follow the steps below:

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 selected as the key K for the cryptographic process.
2. The Application Cryptogram returned in the response to the first GENERATE AC command (the one transmitted in the request message) is copied to a 8-byte field to generate R:

   R := Application Cryptogram

For both the session key used to generate and verify the Application Cryptogram and the ARPC for CVN 18 and CVN '22', and the one for secure messaging, follow the remaining steps below:

3. The third leftmost byte of R is replaced with the value 'F0' to generate F1:

   F1 = R0 || R1 || 'F0' || R3 || R4 || R5 || R6 || R7.

   Session Key A is generated by performing a Triple DEA encipherment of F1 with the key K.
4. The third leftmost byte of R is replaced with the value '0F' to generate F2:

   F2 = R0 || R1 || '0F' || R3 || R4 || R5 || R6 || R7.

   Session Key B is generated by performing a Triple DEA encipherment of F2 with the key K.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.8 Host Security Modules (HSM)

A host (or hardware) security module (HSM) is a specialized 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.8.1 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.7.
- 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 for CVN 10 are described in section D.3.2 and section D.3.3 and for CVN 18 are described in section D.4.2 and section D.4.3.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

D.8.2 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.7.
- 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.7.
- 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.7.
- 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 *EMV 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 *EMV 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E Profiles Functionality

This appendix describes the optional new feature, Profiles Functionality, that allows the issuer to configure the application to use different data values, and perform different application behaviors for different transaction environments. It is optional for the application to be capable of Profiles Functionality; and if the application is capable of Profiles Functionality, it is also optional for an issuer whether to use the Profiles Functionality.

The different transaction environments are typically defined by the issuer based on different values for selected data elements sourced from the terminal, but may also be based on values for a limited set of internal card data elements.

A “Profile” is a set of application behaviors and data elements that are used for processing transactions in a specified transaction environment.

If Profiles Functionality is supported (see conditions in section E.1.1), the issuer can configure the application to:

- return the Processing Options Data Object List (PDOL) in the SELECT AID response to request the values for terminal-sourced data elements that identify the specific terminal transaction environments
- use the data received from the terminal in the GET PROCESSING OPTIONS command, internal card data, simple logic in the application, and rules personalized on the card to choose from several possible profiles supported by the application
- prepare the profile-specific data and behavior the issuer wants used for a given transaction environment so that the card uses the specific data and behavior associated with the Profile selected for a specific transaction.

See section E.2.2 for default application behavior when the application is capable of Profiles Functionality, but the issuer does not personalize the application to support Profiles Functionality.

The two main components of Profiles Functionality are:

- Profile Selection - choosing which profile to use for a specific transaction
- Profile Behavior - choosing what data and behavior are used depending on the chosen profile.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.1 Profile Selection

Profiles Functionality is supported if both of the following are true:

- the application is capable of the Profiles Functionality
- the Profile Selection File is personalized.

If Profiles Functionality is supported, the application shall perform Profile Selection as described in this Appendix.

The application shall use the PDOL to request that the terminal send in the GET PROCESSING OPTIONS (GPO) command data field the data needed for Profile Selection. The application builds the Profile Selection Input Data (to use as the input data for the Profile Selection logic) as described in section E.1.1 from the following:

- an internal data value called the Profile Selection Diversifier (PSD)
- the value portion of the GPO command data (i.e., excluding the Command Template tag '83' and the length of the command data).

The application then uses the Profile Selection Input Data, simple logic in the application, and rules personalized by the issuer in the Profile Selection File to choose whether to respond to the GPO command with an error, or to select which Profile to use for processing the transaction.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.1.1 Building Profile Selection Input Data

The Profile Selection Input Data shall be constructed as follows:

1. The application determines the value for the Profile Selection Diversifier (PSD), which is a one-byte value that identifies application- or transaction-specific internal card data that may be used in choosing the Profile. If there is no internal card data available for use in choosing a Profile, the default value for the PSD should be '00'.

   Note: *The coding of the PSD is at the discretion of the card manufacturer. Examples of internal card data that a vendor might choose to associate with a value in the PSD for use in Profile Selection include:*

   – *on a multi-application card, the PSD may indicate which AID was used to select the application, with the vendor specifying that:*

   - *the first AID personalized on the card is associated with PSD = '01'*
   - *the second AID personalized on the card is associated with PSD = '02'*
   - *the third AID personalized on the card is associated with PSD = '03'*

   – *on a dual-interface card, which physical interface (contact or contactless) is used for the transaction (allowing an issuer to ensure VIS is never used over the contactless interface), with the vendor specifying that:*

   - *if the contact interface is used, bit 8 of the PSD = 0b.*
   - *if the contactless interface is used, bit 8 of the PSD = 1b.*

2. The application extracts the value portion of the GPO command data field (that is, excluding the '83' tag and length for tag '83').
3. The result of concatenating the PSD (from step 1) followed by the value portion of the GPO command data field (from step 2) is called the Profile Selection Input Data (see Figure E-1).

Figure E-1: Profile Selection Input Data

E.1.2 Profile Selection Entries

Each Profile supported by the application is identified by a Profile Identifier (Profile ID). The simple logic in the application follows the rules personalized by the issuer in the Profile Selection File to choose the Profile ID that identifies the profile used for a specific transaction environment.

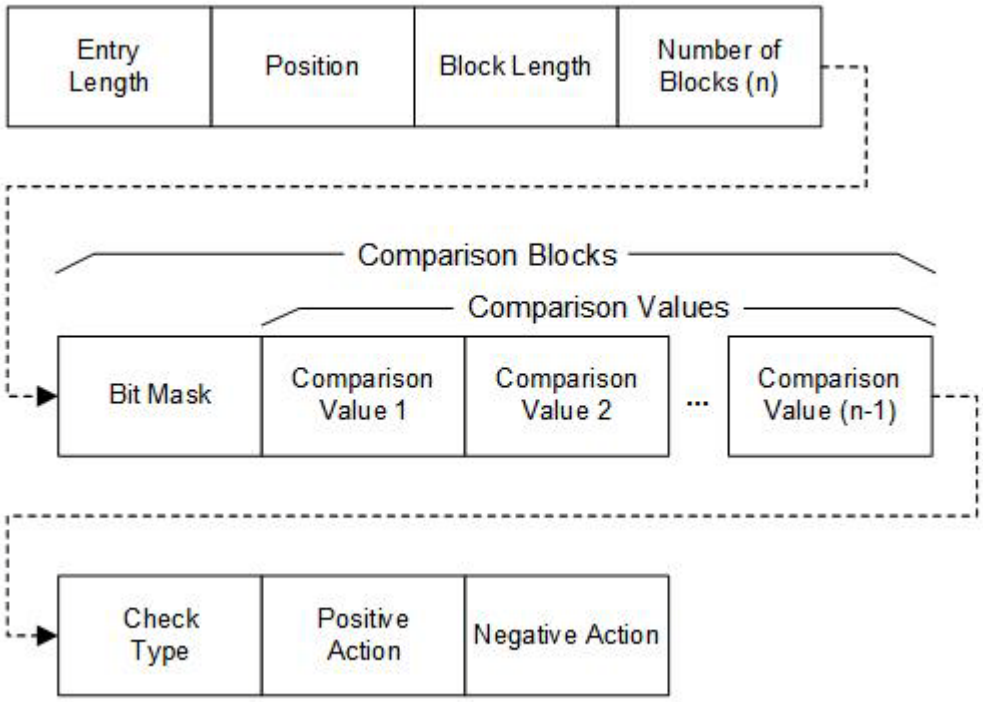
Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The Profile Selection File is a variable length file consisting of a variable number of records, called Profile Selection Entries.

Each Profile Selection Entry is variable length, and contains the rules needed for the application to perform one step in the logic process for selecting the Profile ID for the transaction. Figure E-2 illustrates the Profile Selection Entry format.

The Profile Selection File Entry data element identifies the SFI in which the Profile Selection File is personalized.

Figure E-2: Profile Selection Entry Format



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

A detailed description of the format of each Profile Selection Entry is as shown in Table E-1.

Table E-1: Data Elements in Profile Selection Entry

Data Element	Length	Description
Entry Length	1	Indicates the length of the Profile Selection Entry (not including Entry Length).
Position in Profile Selection Input Data (Position)	1	Indicates the starting position (in bytes) of the portion of Profile Selection Input Data that isused as extracted data input for processing this Profile Selection Entry. If the first byte of Profile Selection Input Data is to be used as the first byte in the extracted data, then the value of Position is '01'. For Check Types that do not use Profile Selection Input Data (for example, Check Types '2x', '3x', '4x', or '52'), Position should be '00'.
Block Length	1	Contains the length of the portion of Profile Selection Input Data that is used as extracted data input for processing a single Profile Selection Entry in the Profile Selection process. It is also the length of each Comparison Value contained in the same Profile Selection Entry. For Check Types that use the value of an application internal data element (such as a counter) instead of using Profile Selection Input Data (for example, Check Types '2x', '3x', '4x', or '52'), Block Length shall be the length of the application internal data element.
Number of Blocks	1	Indicates the number of Comparison Blocks in the Profile Selection Entry. The first Comparison Block is a Bit Mask. The second and subsequent Comparison Blocks are Comparison Value(s) that are compared to the data extracted from the Profile Selection Input Data.
Comparison Blocks	var.	Contains the concatenation of the Bit Mask and one or more Comparison Values.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table E-1: Data Elements in Profile Selection Entry

Data Element	Length	Description	
	Block Length	Bit Mask	Used to mask the extracted data to allow only selected portions of the extracted data to be used as input for processing the Profile Selection Entry (for example, the comparison may be made with only a few bits of a byte). The first Comparison Block is always considered a Bit Mask, but the Bit Mask is only used on data extracted from the Profile Selection Input Data (resulting in "masked extracted data"). See section E.1.3 for details on which checks use the masked extracted data. Each bit whose value is to be used in the comparison shall be set to 1b. Each bit whose value is not used in the comparison shall be set to 0b.
	Block Length	Comparison Value x	Each Comparison Value x contains a value to be compared either to the value of application internal data (for Check Types '2x', '3x', '4x', and '52') or to the masked data extracted from the Profile Selection Input Data (for Check Types '00'and '02').

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table E-1: Data Elements in Profile Selection Entry

Data Element	Length	Description
Check Type	1	Identifies the type of test to be performed using masked data extracted from the Profile Selection Input Data, internal application data, or the Comparison Value(s) in the Profile Selection Entry, as determined by the Check Type. The Check Types that may be supported are: • **'00' = Input Matches Comparison Value(s)** Tests whether the masked value extracted from the Profile Selection Input Data is **equal to** the value of any of the Comparison Values in this Profile Selection Entry. • **'02' = Input Greater Than Comparison Value 1** Tests whether the masked value extracted from the Profile Selection Input Data is **greater than** the value of Comparison Value 1. • **'1x' = Input Greater Than CTTA x Funds** Tests whether the masked value extracted from the Profile Selection Input Data is **greater than** the CTTA x Funds: Cumulative Total Transaction Amount Upper Limit (CTTAUL x) minus Cumulative Total Transaction Amount (CTTA x). • **'2x' = CTC x Greater Than Comparison Value 1** Tests whether Consecutive Transaction Counter x is **greater than** Comparison Value 1. • **'3x' = CTCI x Greater Than Comparison Value 1** Tests whether Consecutive Transaction Counter International x is **greater than** Comparison Value 1. • **'4x' = CTCIC x Greater Than Comparison Value 1** Tests whether Consecutive Transaction Counter International Country x is **greater than** Comparison Value 1. • **'51' = Input Greater Than VLP Available Funds** Tests whether the masked value extracted from the Profile Selection Input Data is **greater than** VLP Available Funds. • **'52' = CLTC Funds Greater Than Comparison Value 1** Tests whether the Contactless Transaction Counter is **greater than** Comparison Value 1.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table E-1: Data Elements in Profile Selection Entry

Data Element	Length	Description
Positive Action	1	Indicates the action to be taken by the application if the Check Type test result is **true**. The Positive Action byte indicates one of the following: • **Profile ID to use for the Transaction** If bit 8 of Positive Action has the value 0b, then the Positive Action byte contains the Profile ID. If Positive Action has the value '7F', then the application will discontinue processing the GPO command and respond with SW1 SW2 = '6985'. • **Number of Profile Selection Entries to Skip** Identifies the number of Profile Selection Entries to skip down in the Profile Selection File for the next Profile Selection Entry to process. If bit 8 of Positive Action has the value 1b, then the Profile Selection algorithm skips down x number of Profile Selection Entries, where x is the value indicated in bits 7-1 of Positive Action.
Negative Action	1	Indicates the action to be taken by the application if the Check Type test result is **false**. The Negative Action byte indicates one of the following: • **Profile ID to use for the Transaction** If bit 8 of Negative Action has the value 0b, then the Negative Action byte contains the Profile ID. If Negative Action has the value '7F', then the application will discontinue processing the GPO command and respond with SW1 SW2 = '6985'. • **Number of Profile Selection Entries to Skip** Identifies the number of Profile Selection Entries to skip down in the Profile Selection File for the next Profile Selection Entry to process If bit 8 of Negative Action has the value 1b, then the Profile Selection algorithm skips down x number of Profile Selection Entries, where x is the value indicated in bits 7-1 of Negative Action.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.1.3 Profile Selection File Processing

The algorithm for processing of a Profile Selection Entry (one step in the processing the Profile Selection File) is illustrated in Figure E-3.

Note: *Applications that support Profiles Functionality can support multiple versions of each type of counter for use in different profiles – referred to as Consecutive Transaction Counter x (CTC x), Consecutive Transaction Counter International x (CTCI x), Consecutive Transaction Counter International Country x (CTCIC x), and Cumulative Total Transaction Amount x (CTTA x). See section E.2.*

The application processes each Profile Selection Entry in the order in which it appears in the Profile Selection File, starting with record 1, as follows:

1. The application extracts a value from the Profile Selection Input Data. The part to be extracted is defined at personalisation using two parameters in the Profile Selection Entry: Position in Profile Selection Input Data (Position) and Block Length.
2. The application masks the extracted value with the Bit Mask (to optionally force some bits to 0b) and then compares the masked value with the values stored in the Profile Selection Entry. This allows for comparison of only a portion of a data element, such as a single bit in Terminal Capabilities.
3. The application performs the test indicated by the Check Type as follows:

   – **Match (Check Type = '00')**

   The application tests whether the value extracted from the Profile Selection Input Data is **equal to** any of the Comparison Value(s) in the Profile Selection Entry.

   - If the masked extracted data matches one or more of the Comparison Value(s), the Positive Action shall be performed.
   - If the masked extracted data does not match any of the Comparison Value(s), the Negative Action shall be performed.

   – **Greater Than (Check Type = '02')**

   The application tests whether the value extracted from the Profile Selection Input Data is **greater than** Comparison Value 1.

   - If the value of the masked extracted data is greater than Comparison Value 1, the Positive Action shall be performed.
   - If the value of the masked extracted data is less than or equal to Comparison Value 1, the Negative Action shall be performed.

   – **Amount Greater Than CTTA Funds (Check Type = '1x')**

   The application tests whether the value extracted from the Profile Selection Input Data is **greater than** the CTTA x Funds (that is, CTTAUL x minus CTTA x; or if CTTAUL x is not present, CTTAL x minus CTTA x).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

- If the value of the masked extracted data is greater than CTTA x Funds, the Positive Action shall be performed.
- If the value of the masked extracted data is less than or equal to CTTA x Funds, the Negative Action shall be performed.

– **CTC x Greater Than Value (Check Type = '2x')**

The application tests whether Consecutive Transaction Counter x (CTC x) is **greater than** Comparison Value 1.

- If CTC x is greater than Comparison Value 1, the Positive Action shall be performed.
- If CTC x is less than or equal to Comparison Value 1, the Negative Action shall be performed.

– **CTCI x Greater Than Value (Check Type = '3x')**

The application tests whether Consecutive Transaction Counter International x (CTCI x) is **greater than** Comparison Value 1.

- If CTCI x is greater than Comparison Value 1, the Positive Action shall be performed.
- If CTCI x is less than or equal to Comparison Value 1, the Negative Action shall be performed.

– **CTCIC x Greater Than Value (Check Type = '4x')**

The application tests whether Consecutive Transaction Counter International Country x (CTCIC x) is **greater than** Comparison Value 1.

- If CTCIC x is greater than Comparison Value 1, the Positive Action shall be performed.
- If CTCIC x is less than or equal to Comparison Value 1, the Negative Action shall be performed.

– **Amount Greater Than VLP Available Funds (Check Type = '51')**

The application tests whether the value extracted from the Profile Selection Input Data is **greater than** VLP Available Funds.

- If the value of the masked extracted data is greater than VLP Available Funds, the Positive Action shall be performed.
- If the value of the masked extracted data is less than or equal to VLP Available Funds, the Negative Action shall be performed.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

– **CLTC Greater Than Value (Check Type = '52')**

The application tests whether Contactless Transaction Counter (CLTC) is **greater than** Comparison Value 1.

- If CLTC is greater than Comparison Value 1, the Positive Action shall be performed.
- If CLTC is less than or equal to Comparison Value 1, the Negative Action shall be performed.

4. The Positive Action or Negative Action is performed as follows:

   If bit 8 has the value 0b, then the Profile ID used for the transaction shall have the value indicated by the (Positive or Negative) Action byte.

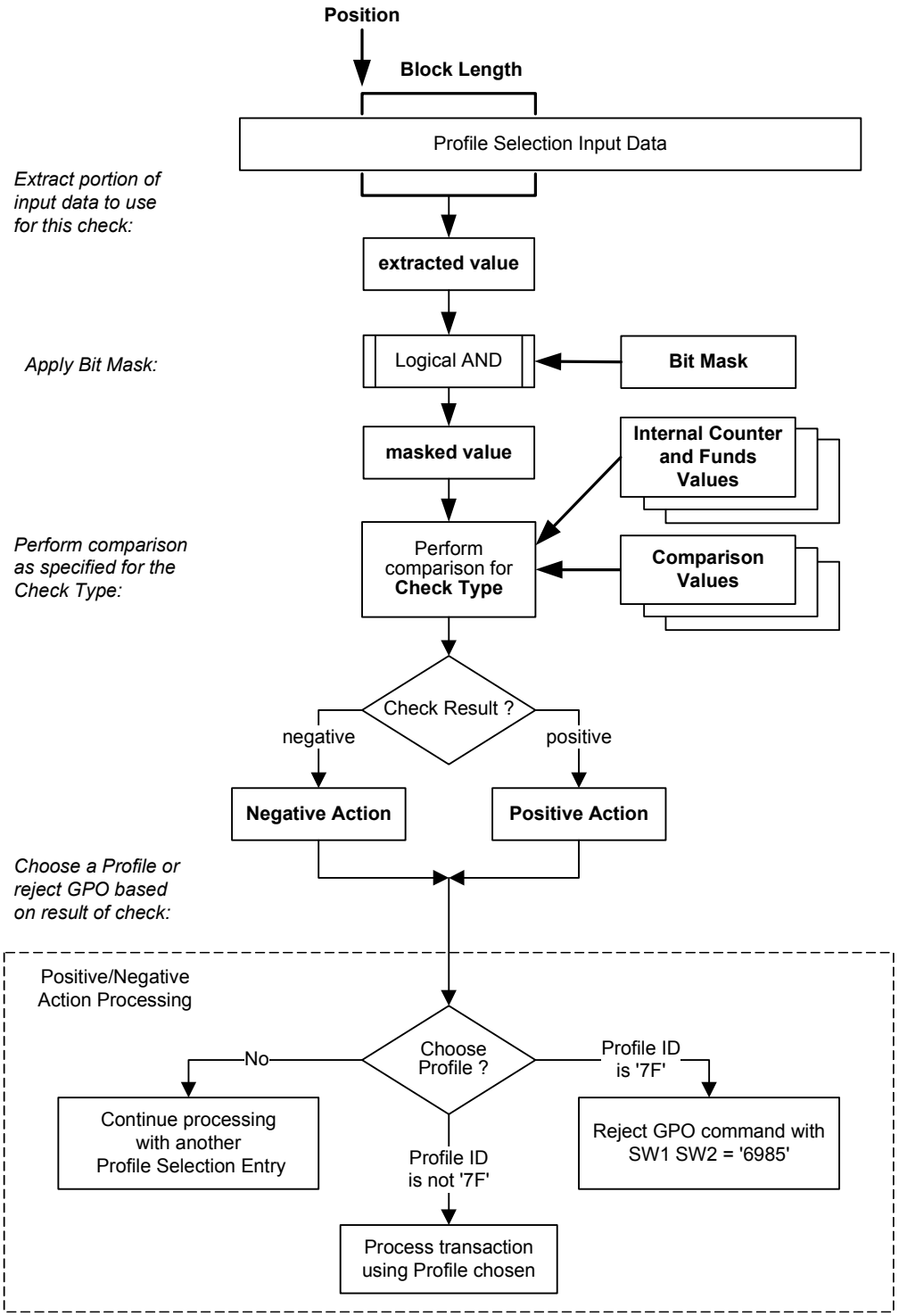
   If bit 8 has the value 1b, then the profile selection algorithm shall skip down x number of Profile Selection Entries, where x is the value indicated in bits 7-1 of the (Positive or Negative) Action byte.

If processing of the Profile Selection Entries does not result in selection of a Profile ID for which a Profile Control is present, then the Profile ID used for the transaction shall be '7F' (used to indicate an error in the GET PROCESSING OPTIONS response).

Note: *If the Profile ID has the value '7F', then there is no valid Profile Control and the application shall discontinue processing the GPO command and shall respond with SW1 SW2 = '6985'.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Figure E-3: Profile Selection Entry Processing Algorithm



Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.1.4 Profile Selection Example

This example shows how the Profile Selection File could be configured to:

- Not allow transactions outside the issuer country
- Select Profile 2 for domestic country transactions at ATMs or attended cash disbursement transactions
- Select Profile 1 for all other domestic country transactions.

Table E-2 lists the profiles.

Table E-2: Profile Selection Example – Profiles

Transaction Environment	Selection Criteria	Profile ID
International country	Terminal Country Code is not = '0036'	'7F' (Error response)
Domestic ATMs and attended cash disbursement terminals	(Terminal Type = '1x') AND (Cash bit = 1b in Additional Terminal Capabilities)	'02'
All other domestic terminals	Doesn't meet the criteria for any other transaction environment	'01'

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The simplified list of Profile Selection Entries in Table E-3 shows that the profiles can be selected with the profile selection algorithm:

Table E-3: Profile Selection Example – Profile Selection File

	Extracted Data	Comparative Value	Check Type	Positive Action	Negative Action
1	Terminal Country Code	'0036'	Match	Skip down 1	Profile ID = '7F' (respond to GPO command with error)
2	Terminal Type	'1x' (using masking)	Match	Skip down 1	Select profile '01'
3	Additional Terminal Capabilities	cash bit = 1b (using masking)	Match	Select profile '02'	Select profile '01'

The PDOL must contain the tags and lengths for the data elements listed in Table E-4. so the PDOL value would be '9F35019F4001'.,

Table E-4: Profile Selection Example – PDOL Contents

Data Element	Tag	Length
Terminal Country Code	'9F1A'	2
Terminal Type	'9F35'	1
Additional Terminal Capabilities	'9F40'	1

Note: *Although the Additional Terminal Capabilities data element is 2 bytes long, the Profile Selection logic only needs the first byte of the data element, so the card requests only the first byte of the data element from the terminal.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The coding of the Profile Selection Entries for this example is shown in Table E-5.

Table E-5: Profile Selection Entries – Complex Example

Profile Selection Entries	Value
Profile Selection Entry 1	'0A 02 02 02 FFFF 0036 00 81 7F'
Profile Selection Entry 2	'08 04 01 02 F0 10 00 81 01'
Profile Selection Entry 3	'08 05 01 02 80 80 00 02 01'

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.2 Profile Behavior

The Profile ID selected during Profile Selection identifies the Profile Control x to be used to configure the application behavior for Initiate Application Processing and Card Action Analysis.

Applications that support Profiles Functionality shall be capable of supporting multiple versions of the AIP, AFL, and each type of counter – Consecutive Transaction Counter (CTC), Consecutive Transaction Counter International (CTCI), Consecutive Transaction Counter International Country (CTCIC), and Cumulative Total Transaction Amount (CTTA) – for use in different profiles. See section E.3 for the minimum number of each type the application must be capable of supporting.

The different AIPs are identified as AIP x, and the different AFLs as AFL x. The AIP number and AFL number for a specific Profile shall match (because both data elements are personalized in a single data element, the AIP/AFL Entry x). AIP/AFL Entry x consists of the concatenation of AIP x, followed by the length of AFL x, followed by the value of AFL x.

Note: *The "x" for AIP/AFL Entry x does not have to match the value of "x" in Profile Control x.*

For example, AIP/AFL Entry x could refer to AIP/AFL Entry 1, AIP/AFL Entry 2, AIP/AFL Entry 3, or AIP/AFL Entry 4; and any of the four AIP/AFL Entry x's could be used in Profile 1 (which uses Profile Control 1).

The AIP/AFL Entry ID in the Profile Control identifies which AIP/AFL Entry x is to be used for transactions conducted in that Profile. For example, if Profile 1 uses AIP/AFL Entry 3, then Profile Control 1 will have AIP/AFL Entry ID = '3'.

The different instances of each type of counter are identified as CTC x, CTCI x, CTCIC x, and CTTA x, where x varies from one to the maximum number of the specified type of each data element supported by the application.

Note: *The "x" for each of these data elements does not have to match the value of "x" in Profile Control x.*

For example, CTC x could refer to CTC 1, CTC 2, CTC 3, or CTC 4; and any of the four CTC x's could be used in Profile 2 (which uses Profile Control 2).

If issuers want to count transactions that use different Profiles separately, then each Profile should use a different counter number. For example, if the application uses CTC 1 in Profile 1, and CTC 2 in Profile 2; then the value in CTC 1 is a count of only transactions that use Profile 1, and the value in CTC 2 is a count of only transactions that use Profile 2.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

If issuers want to count transactions that use different profiles all in one counter, then each Profile should use the same counter number. For example, if the application uses CTC 1 in Profile 1, Profile 2, and Profile 3; then the value in CTC 1 is a count of all transactions that are performed using any of the 3 Profiles.

The following data and application behavior are profile-specific:

- AIP and AFL values returned in the GPO response
  - The AIP allows the application to indicate the forms of offline data authentication supported for each profile
  - The AFL allows different record data to be read by the terminal for different profiles (for example, different Cardholder Verification Method Lists, lower and upper limits for terminal velocity checking, or different SDA signatures)
- The following options in the ADA (if Profiles Functionality is supported, the setting for each of these options in the Profile Control x chosen for the Profile is used instead of the setting in the ADA):
  - If Issuer Authentication failure, transmit next transaction online
  - If new card, transmit transaction online
  - If new card, decline if unable to transmit transaction online
  - If PIN Try Limit exceeded on previous transaction, transmit transaction online
  - If Issuer Script failed on a previous transaction, transmit transaction online
- Whether to log transactions that are performed using the profile (if transaction logging is supported).
- Which velocity-checking counters may be incremented for offline transactions
  - Each instance of a counter can be configured by the issuer to be incremented in only a single profile, or shared across multiple profiles.
  - Some counters may not be used in any profile.
  - Each instance of a counter that is active for a profile is only incremented if the conditions for incrementing the counter are met (for example, the Consecutive Transaction Counter International Country (CTCIC) does not increment if the transaction is not conducted outside the Issuer Country).
- Which velocity-checking counters are to be checked against their associated lower and upper limits during card risk management
  - Every counter that is allowed to increment in the profile shall be checked against the associated limits.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - Any counter that is not allowed to increment in a profile may also be checked against the associated limits (for example, the card may have a counter that only increments for low value transactions, but the issuer may want the card to check whether the low-value counter has exceeded its lower limit even though the transaction is being processed using a Profile for high-value transactions).

- Which velocity-checking counters may be reset after online approved transactions that meet the issuer authentication requirements
  - The counters may be reset to zero to allow more transactions to be approved offline.
  - The counters may be set to the associated upper limit so that transactions may no longer be approved offline.

E.2.1 Using the Profile Control

Profile-specific data and behaviors are configured in a Profile Control x data element (see for a detailed description).

The Profile Control used for a transaction is Profile Control x, where x = the Profile ID chosen for the transaction during Profile Selection.

The Profile-specific data and behaviors are configured as follows:

- The AIP and AFL to be used for the transaction are in the AIP/AFL Entries x data element, where x = the AIP/AFL Entry ID in the Profile Control for the transaction.
- The application uses the setting of the ‘If Issuer Authentication failure, transmit next transaction online’, ‘If new card, transmit transaction online’, ‘If new card, decline if unable to transmit transaction online’, ‘If PIN Try Limit exceeded on previous transaction, transmit transaction online’, and ‘If Issuer Script failed on a previous transaction, transmit transaction online’ bits in the Profile Control chosen for the transaction instead of the corresponding bits in the ADA:
- The application uses the ‘Log transaction performed using this profile’ bit in the Profile Control to determine whether the transaction may be logged.
  - If the bit is set to 0b, transactions shall not be logged.
  - If the bit is set to 1b, transactions are logged if they meet the other conditions for logging transactions (for example, if the application only logs approved transactions, a declined transaction would not be logged even though the bit is set to 1b).
- For each Consecutive Transaction Counter x (CTC x) supported by the application:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - CTC x is checked against its corresponding lower limit – Consecutive Transaction Counter Limit (CTCL x) – and upper limit – Consecutive Transaction Counter Upper Limit (CTCUL x) – during GENERATE AC command processing only if either the 'Allow counting in CTC x' bit of the Profile Control is set to 1b, or the 'Check limits for CTC x' bit of the Profile Control is set to 1b.
  - CTC x may only be incremented if the 'Allow counting in CTC x' bit of the Profile Control is set to 1b (other conditions for incrementing a CTC also apply).
  - CTC x may be reset during GENERATE AC command processing only if the 'Allow reset of CTC x' bit of the Profile Control is set to 1b.

- For each Consecutive Transaction Counter International x (CTCI x) supported by the application:
  - CTCI x is checked against its corresponding lower limit – Consecutive Transaction Counter International Limit (CTCIL x) – and upper limit – Consecutive Transaction International Upper Limit (CTIUL x) – during GENERATE AC command processing only if either the 'Allow counting in CTCI x' bit of the Profile Control is set to 1b, or the 'Check limits for CTCI x' bit of the Profile Control is set to 1b.
  - CTCI x may only be incremented if the 'Allow counting in CTCI x' bit of the Profile Control is set to 1b (other conditions for incrementing a CTCI also apply).
  - CTCI x may be reset during GENERATE AC command processing only if the 'Allow reset of CTCI x' bit of the Profile Control is set to 1b.
- For each Consecutive Transaction Counter International Country x (CTCIC x) supported by the application:
  - CTCIC x is checked against its corresponding lower limit – Consecutive Transaction Counter International Country Limit (CTCICL x) – and upper limit – Consecutive Transaction International Upper Limit (CTIUL x) – during GENERATE AC command processing only if either the 'Allow counting in CTCIC x' bit of the Profile Control is set to 1b, or the 'Check limits for CTCIC x' bit of the Profile Control is set to 1b.
  - CTCIC x may only be incremented if the 'Allow counting in CTCIC x' bit of the Profile Control is set to 1b (other conditions for incrementing a CTCIC also apply).
  - CTCIC x may be reset during GENERATE AC command processing only if the 'Allow reset of CTCIC x' bit of the Profile Control is set to 1b.
- For each Cumulative Total Transaction Amount x (CTTA x) supported by the application:

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

  - CTTA x is checked against its corresponding lower limit – Cumulative Total Transaction Amount Limit (CTTAL x) – and upper limit – Cumulative Total Transaction Amount Upper Limit (CTTAUL x) – during GENERATE AC command processing only if either the ‘Allow counting in CTTA x’ bit of the Profile Control is set to 1b, or the ‘Check limits for CTTA x’ bit of the Profile Control is set to 1b.
  - CTTA x may only be incremented if the ‘Allow counting in CTTA x’ bit of the Profile Control is set to 1b (other conditions for incrementing a CTTA also apply).
  - CTTA x may be reset during GENERATE AC command processing only if the ‘Allow reset of CTTA x’ bit of the Profile Control is set to 1b.

- If the Contactless Transaction Counter (CLTC) is supported by the application:
  - CLTC is checked against its corresponding lower limit (CLTCLL) during GENERATE AC command processing only if the ‘Check limits for CLTC’ bit of the Profile Control is set to 1b.

    Note: *CLTC is not incremented for contact transactions.*
  - CLTC may be reset during GENERATE AC command processing only if the ‘Allow reset of CLTC’ bit of the Profile Control is set to 1b.
- If the VLP Available Funds is supported by the application:
  - VLP Available Funds is checked against its corresponding limit (VLP Reset Threshold) during GENERATE AC command processing only if the ‘Check limits for VLP Available Funds’ bit of the Profile Control is set to 1b.

    Note: *VLP Available Funds is not incremented for contact transactions.*
  - VLP Available Funds may be reset during GENERATE AC command processing only if the ‘Allow reset of VLP Available Funds’ bit of the Profile Control is set to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.2.2 Default Application Behavior for Profiles Functionality

If the application is capable of Profiles Functionality, but the Profile Selection File is not present, the application shall not use Profiles Functionality, and shall configure the application data and behavior as follows:

- The conditions for managing counters are not dependent on options in a Profile Control
- Only one of each type of counter (one Cumulative Total Transaction Amount (CTTA), one Consecutive Transaction Counter (CTC), one Consecutive Transaction Counter International (CTCI), and one Consecutive Transaction Counter International Country (CTCIC)) may be used by the application
  - If the Limit or Upper Limit for any counter is personalized using a primitive tag ('9Fxx'), then the value associated with the primitive tag shall be used for the associated counter. Otherwise the value personalized in the Counters Data or Amounts Data templates for instance x=1 of each type of counter is used as the limit. That is:
    - If tag '9F58' is personalized, then the CTCL has the value for tag '9F58'. Otherwise, CTCL has the value for tag 'DF21' in 'BF56'.
    - If tag '9F59' is personalized, then the CTCUL has the value for tag '9F59'. Otherwise, CTCUL has the value for tag 'DF31' in 'BF56'.
    - If tag '9F53' is personalized, then the CTCIL has the value for tag '9F53'. Otherwise, CTCIL has the value for tag 'DF21' in 'BF57'.
    - If tag '9F5E' is personalized, then the CTIUL has the value for tag '9F5E'. Otherwise, CTIUL has the value for tag 'DF31' in 'BF57'.
    - If tag '9F72' is personalized, then the CTCICL has the value for tag '9F72'. Otherwise, CTCICL has the value for tag 'DF61' in 'BF57'.
    - If tag '9F54' is personalized, then the CTTAL has the value for tag '9F54'. Otherwise, CTTAL has the value for tag 'DF21' in 'BF58'.
    - If tag '9F5C' is personalized, then the CTTAUL has the value for tag '9F5C'. Otherwise, CTTAUL has the value for tag 'DF31' in 'BF58'.
- The application uses bits in the Application Default Action (ADA) to determine issuer options (instead of the profile-specific ADA options in any Profile Control x)
- If the AIP and AFL are personalized using tags '82' and '94' respectively, then the application uses the AIP ('82') and AFL ('94') when building the GET PROCESSING OPTIONS response, otherwise the application builds the GET PROCESSING OPTIONS response using AIP/AFL Entry 1 (tag 'DF11' in template 'BF5A').

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

E.3 Minumum Support for Profiles Functionality

Applications that are capable of Profiles Functionality shall be able to support at least four Profile Controls (Profile Control 1, Profile Control 2, Profile Control 3, and Profile Control 4), although issuers may choose to use fewer than four Profile Controls.

Note: *Applications may support more than four Profile Controls, at implementer discretion.*

Applications that are capable of Profiles Functionality shall be able to support at least four AIP/AFL Entries, each of which contains a TLV-coded AIP and AFL (AIP/AFL Entry 1 contains AIP 1 and AFL 1, AIP/AFL Entry 2 contains AIP 2 and AFL 2, AIP/AFL Entry 3 contains AIP 3 and AFL 3, and AIP/AFL Entry 4 contains AIP 4 and AFL 4), although issuers may choose to use fewer than four AIP/AFL Entries.

Note: *Applications may support more than four AIP/AFL Entries, at implementer discretion.*

Applications that are capable of Profiles Functionality shall be able to support at least four Consecutive Transaction Counters (CTC 1, CTC 2, CTC 3, and CTC 4), although issuers may choose to use fewer than four CTCs.

Note: *Applications may support more than four CTCs, at implementer discretion.*

Applications that are capable of Profiles Functionality shall be able to support at least four Consecutive Transaction Counters International (CTCI 1, CTCI 2, CTCI 3, and CTCI 4), although issuers may choose to use fewer than four CTCIs.

Note: *Applications may support more than four CTCIs, at implementer discretion.*

Applications that are capable of Profiles Functionality shall be able to support at least four Consecutive Transaction Counters International Country (CTCIC 1, CTCIC 2, CTCIC 3, and CTCIC 4), although issuers may choose to use fewer than four CTCICs.

Note: *Applications may support more than four CTCICs, at implementer discretion.*

Applications that are capable of Profiles Functionality shall be able to support at least four Cumulative Total Transaction Amounts (CTTA 1, CTTA 2, CTTA 3, and CTTA 4), although issuers may choose to use fewer than four CTTAs.

Note: *Applications may support more than four CTTAs, at implementer discretion.*

Note: *The Profile Control x data element may be extended to support controls for additional counters, but such functionality is beyond the scope of this specification.*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

F Issuer Application Data and Card Verification Results Formats

This appendix defines two formats of Issuer Application Data (IAD):

- IAD Format 0/1/3
- IAD Format 2

The IAD Format is indicated in the left nibble of the CVN value, and indicates the layout of the Issuer Application Data, such as the length of the IAD, the format of the CVR, and where to find the Derivation Key Index (DKI) and Issuer Discretionary Data Option ID.

This appendix includes the following sections:

F.1 Issuer Application Data (IAD) Formats

F.2 Card Verification Results (CVR) Format for IAD Formats

F.3 Determining the IAD Format

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

F.1 Issuer Application Data (IAD) Formats

Table F-1: IAD Formats (1 of 2)

Byte	IAD Format 0/1/3 (Current)	IAD Format 2 *(New in VIS 1.6)*
1	Length of Visa Discretionary Data = '06' (6)	Length of IAD = '1F' (31)
2	DKI	CVN (left nibble = IAD forma ***Note:*** *The only values supported are '22' and '2C'.*
3	CVN	DKI
4	CVR byte 1 (= CVR Length = '03')	CVR byte 1 (bitmap RFU)
5	CVR byte 2 (bitmap)	CVR byte 2 (bitmap – same as for VIS Format 0/1/3)
6	CVR byte 3 (bitmap)	CVR byte 3 (bitmap – same as for VIS Format 0/1/3)
7	CVR byte 4 (bitmap)	CVR byte 4 (bitmap – same as for VIS Format 0/1/3)
8	Length of Issuer Discretionary Data (optional)	CVR byte 5 (bitmap RFU)
9	Issuer Discretionary Data (optional) (optional: Right nibble = Issuer Discretionary Data Option ID)	Left nibble = RFU Right nibble = Issuer Discretionary Data Option ID
10	Issuer Discretionary Data (optional)	Issuer Discretionary Data
11	Issuer Discretionary Data (optional)	Issuer Discretionary Data
12	Issuer Discretionary Data (optional)	Issuer Discretionary Data
13	Issuer Discretionary Data (optional)	Issuer Discretionary Data
14	Issuer Discretionary Data (optional)	Issuer Discretionary Data
15	Issuer Discretionary Data (optional)	Issuer Discretionary Data
16	Issuer Discretionary Data (optional)	Issuer Discretionary Data
17	Issuer Discretionary Data (optional)	Issuer Discretionary Data
18	Issuer Discretionary Data (optional)	Issuer Discretionary Data
19	Issuer Discretionary Data (optional)	Issuer Discretionary Data
20	Issuer Discretionary Data (optional)	Issuer Discretionary Data
21	Issuer Discretionary Data (optional)	Issuer Discretionary Data
22	Issuer Discretionary Data (optional)	Issuer Discretionary Data
23	Issuer Discretionary Data (optional)	Issuer Discretionary Data

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table F-1: IAD Formats (2 of 2)

Byte	IAD Format 0/1/3 (Current)	IAD Format 2 *(New in VIS 1.6)*
24	--- not available ---	Issuer Discretionary Data
25	--- not available ---	Issuer Discretionary Data
26	--- not available ---	Issuer Discretionary Data
27	--- not available ---	Issuer Discretionary Data
28	--- not available ---	Issuer Discretionary Data
29	--- not available ---	Issuer Discretionary Data
30	--- not available ---	Issuer Discretionary Data
31	--- not available ---	Issuer Discretionary Data
32	--- not available ---	Issuer Discretionary Data

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

F.2 Card Verification Results (CVR) Format for IAD Formats

Table F-2: Card Verification (CVR) Formats for IAD Format 0/1/3 and IAD Format 2 (1 of 2)

Byte/bit	CVR for IAD Format 0/1/3 (Current)	CVR for IAD Format 2 *(New in VIS 1.6)*
1 / 8-1	CVR Length = fixed hex '03'	RFU
2 / 8-7	Cryptogram Type in second GENERATE AC 00b = AAC returned in second GENERATE AC 01b = TC returned in second GENERATE AC 10b = second GENERATE AC not requested 11b = RFU	Cryptogram Type in second GENERATE AC 00b = AAC returned in second GENERATE AC 01b = TC returned in second GENERATE AC 10b = second GENERATE AC not requested 11b = RFU
2 / 6-5	Cryptogram Type in first GENERATE AC 00b = AAC returned in first GENERATE AC 01b = TC returned in first GENERATE AC 10b = ARQC returned in first GENERATE AC 11b = RFU	Cryptogram Type in first GENERATE AC 00b = AAC returned in first GENERATE AC 01b = TC returned in first GENERATE AC 10b = ARQC returned in first GENERATE AC 11b = RFU
2 / 4	Issuer Authentication performed and failed	Issuer Authentication performed and failed
2 / 3	Offline PIN verification performed	Offline PIN verification performed
2 / 2	Offline PIN verification failed	Offline PIN verification failed
2 / 1	Unable to go online	Unable to go online
3 / 8	Last online transaction not completed	Last online transaction not completed
3 / 7	PIN Try Limit exceeded	PIN Try Limit exceeded
3 / 6	Exceeded velocity checking counters	Exceeded velocity checking counters
3 / 5	New card	New card
3 / 4	Issuer Authentication failure on last online transaction	Issuer Authentication failure on last online transaction
3 / 3	Issuer Authentication not performed after online authorization	Issuer Authentication not performed after online authorization
3 / 2	Application blocked by card because PIN Try Limit exceeded	Application blocked by card because PIN Try Limit exceeded
3 / 1	Offline static data authentication failed on last transaction and transaction declined offline	Offline static data authentication failed on last transaction and transaction declined offline
4 / 8-5	Number of Issuer Script commands	Number of Issuer Script commands
4 / 4	Issuer Script processing failed	Issuer Script processing failed

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table F-2: Card Verification (CVR) Formats for IAD Format 0/1/3 and IAD Format 2 (2 of 2)

Byte/bit	CVR for IAD Format 0/1/3 (Current)	CVR for IAD Format 2 *(New in VIS 1.6)*
4 / 3	Offline dynamic data authentication failed on last transaction and transaction declined offline	Offline dynamic data authentication failed on last transaction and transaction declined offline
4 / 2	Offline dynamic data authentication performed	Offline dynamic data authentication performed
4 / 1	PIN verification command not received for a PIN-Expecting card	PIN verification command not received for a PIN-Expecting card
5 / 8	--- not available ---	RFU
5 / 7	--- not available ---	RFU
5 / 6	--- not available ---	RFU
5 / 5	--- not available ---	RFU
5 / 4	--- not available ---	RFU
5 / 3	--- not available ---	RFU
5 / 2	--- not available ---	CDCVM Successfully Performed
5 / 1	--- not available ---	Secure Messaging uses EMV Session key-based derivation

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

F.3 Determining the IAD Format

An issuer host can determine the format of the Issuer Application Data as follows:

1. If the first byte has the value '06', then:
   - the Issuer Application Data complies with IAD Format 0/1/3
   - the CVN is in Byte 3 of the Issuer Application Data
   - the DKI is in Byte 2 of the Issuer Application Data
2. If the first byte has the value '1F', then:
   - the CVN is in Byte 2 of the Issuer Application Data, and the left nibble of the CVN indicates the IAD Format, as described in this appendix.
   - the location of the DKI is determined based on the IAD Format. For IAD Format 2, the DKI is in Byte 3 of the Issuer Application Data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

G Overview of Velocity-Checking Counters

This appendix provides an overview of the different counters used in VIS for velocity-checking, and identifies the limits associated with each counter.

Lower Limit — the value at which the issuer wants the card to begin to try to go online to reset offline counters.

Upper Limit — the maximum amount that the cardholder may spend offline or the maximum number of offline transactions that may be performed before the card must go online for authorization (or decline offline).

Type — identifies whether the counter tracks amounts (which are tracked in the designated application currency, but may contain approximate value of amounts converted from other currencies) or a count of the number of transactions.

Counts — identifies whether the counter increments (counts up, nominally from zero) or decrements (counts down, nominally from an upper limit).

Profiles — identifies whether there are multiple instances of this type of counter or only one instance of the counter if Profiles Functionality is supported.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table G-1: Velocity-checking Counters Used in VIS

Counter Name	Counter Lower Limit	Counter Upper Limit	Type	Counts	Profiles
Cumulative Total Transaction Amount (CTTA)	Cumulative Total Transaction Amount Limit (CTTAL)	Cumulative Total Transaction Amount Upper Limit (CTTAU)	Amount	Up	Multiple
Consecutive Transaction Counter (CTC)	Consecutive Transaction Counter Limit (CTCL)	Consecutive Transaction Counter Upper Limit (CTCUL)	Count	Up	Multiple
Consecutive Transaction Counter International (CTCI)	Consecutive Transaction Counter International Limit (CTCIL)	Consecutive Transaction International Upper Limit (CTIUL) ***Note:*** *This same limit is also used by the CTCIC.*	Count	Up	Multiple
Consecutive Transaction Counter International Country (CTCIC)	Consecutive Transaction Counter International Country Limit (CTCICL)	Consecutive Transaction International Upper Limit (CTIUL) ***Note:*** *This same limit is also used by the CTCI.*	Count	Up	Multiple
Contactless Transaction Counter (CLTC)	Contactless Transaction Counter Lower Limit (CLTCLL)	Contactless Transaction Counter Upper Limit (CLTCUL)	Count	Up	One
VLP Available Funds	VLP Reset Threshold	VLP Funds Limit	Amount	Down	One

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

G.1 Counter Overflow

Counters shall not be incremented above their maximum possible value (an overflow) and shall not be decremented below zero.

If increment of a counter would result in an overflow, then the application shall set the counter to the maximum possible value (for example, the CTC would be set to 'FF', the CTTA would be set to '99 99 99 99 99 99').

If decrement of a counter would result in a value less than zero, then the application shall set the counter to a value of zero.

For the evaluation of conditions, if incrementing a counter would result in an overflow or decrementing a counter would cause a negative value to be used for the comparison, then the result of the comparison shall be that velocity checking counters were exceeded.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

H Dual-Interface Contactless and Contact

The Visa Contactless Payment Specification (VCPS) defines requirements for conducting a payment transaction over a contactless interface. The quick VSDC (qVSDC) path in VCPS mostly relies on online authorized contact chip transactions to update offline counters. A dual-interface card supporting both qVSDC and VIS requires a few additional functionalities in the contact functionality to address the needs of the qVSDC functionality.

For dual-interface cards that support both qVSDC and VIS, this section identifies the new functionality added to VIS to address the needs of the qVSDC functionality.

This appendix includes the following sections:

H.1 Common Data

H.2 Data Accessibility

H.3 New Functionality by Section

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

H.1 Common Data

See VCPS Appendix D for information regarding which data elements are shared between VIS and VCPS.

H.2 Data Accessibility

This section outlines the requirements for the accessibility of contact-exclusive data, contactless-exclusive data, and shared data.

H.2.1 Record Data Restricted by Interface

Records that are only listed in the Application File Locator(s) used for the contactless interface, shall not be accessible over the contact interface.

Records that are only listed in AFL(s) used for the contact interface shall not be accessible over the contactless interface.

Records that are not listed in any AFL should be accessible over the contact interface and shall not be accessible over the contactless interface. This excludes transaction log records, whose accessibility is described in section H.2.2.

If the record requested by the READ RECORD command is not allowed to be retrieved over the interface, the card responds with an error SW1 SW2 ('6A83' is recommended).

If the application supports Profiles Functionality over the contact interface, then a record listed in any of the AFL x's in the AIP/AFL Entries template may be retrieved over the contact interface.

For example, a record present only in the AFL for the qVSDC path in VCPS shall only be accessible over the contactless interface, and a record present in the AFL for both qVSDC and VIS shall be accessible over both the contactless and contact interfaces.

Note: *This record retrieval restriction is based only on whether the record was personalized in the AFL for the card paths, regardless of whether or not the AFL was returned by the card prior to the card application receiving the READ RECORD command. Issuers shall (using the AFLs) be able to configure any record to be accessible over only the contact interface, only the contactless interface, or both interfaces.*

H.2.2 Transaction Log Records Restricted by Interface

If transaction logging is implemented, then the Transaction log records shall be issuer configurable to be accessible over the contact interface-only, over the contactless interface-only, or over both interfaces.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

H.2.3 Application Internal Data Elements

GET DATA:

- VIS (Table A-1) defines whether card internal data elements are retrievable by the GET DATA command over the contact interface.
- VCPS (Table D-1) defines whether card internal data elements are retrievable by the GET DATA command over the contactless interface.
- Card internal data objects defined in VIS but not defined in VCPS *shall not* be retrievable by the GET DATA command over the contactless interface.
- Card internal data objects defined in VCPS but not defined in VIS *should* be retrievable by the GET DATA command over the contact interface.

PUT DATA:

- Card internal data objects defined in VCPS Table D-1 as updatable by the PUT DATA command shall be updatable by the PUT DATA command received over the contact interface (if the PUT DATA command is supported for contact and the data element is present in the application).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

H.3 New Functionality by Section

H.3.1 Initiate Application Processing (Chapter 4)

The Last Contactless Application Cryptogram Valid Indicator is reset when a VIS transaction is in itiated.

H.3.2 First GENERATE AC Command Verification (Chapter 11)

If the card sends Issuer Discretionary Data in an ARQC response using an option that includes the Available Offline Spending Amount, then the method for calculating the Available Offline Spending Amount will depend on which low value option is supported for contactless transactions, as identified in the CAP data element shared with the contactless functionality.

If the contactless functionality uses the Contactless Transaction Counter (CLTC) or the VLP Available Funds for contactless transactions, then the card will check whether contact transactions should attempt to go online (so that contactless counters could be reset) because contactless funds are low.

For the Low value AND CTTA option for contactless, it is possible to reset the VLP Available Funds to the VLP Funds Limit with a successful PIN verification over the contact interface. This behavior is controlled by ADA byte 3 bit 5, which if set means that the VLP Available Funds shall be reset to the VLP Funds Limit whenever the offline PIN is successfully verified, the card is not a new card, and the transaction is approved.

H.3.3 Second GENERATE AC Command Verification (Chapter 13)

Cumulative Total Transaction Amount (CTTA), which may also be used by the contactless functionality, is reset after an online approval if the issuer authentication requirements are met and the ADA does not indicate that CTTA is to be reset by issuer script processing instead of during GENERATE AC processing.

VLP Available Funds is reset after an online approval if the issuer authentication requirements are met and the ADA does not indicate that VLP Available Funds is to be reset by issuer script processing instead of during GENERATE AC processing.

If the contactless functionality uses the Contactless Transaction Counter (CLTC) or the VLP Available Funds for contactless transactions, then the card will check whether an online response to a contact transaction meets the requirements to allow the contactless counters to be reset.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The contactless functionality may be disabled at the time of personalization or by a PUT DATA command. Issuers may choose either to allow the application to automatically re-enable contactless functionality with an online approved transaction, or to restrict enabling of the contactless functionality to a successful issuer script command. During second GENERATE AC processing, if the transaction was approved online, issuer authentication requirements are met, and the issuer allows the application to enable contactless functionality automatically after an online approved transaction; then the application will re-enable contactless functionality.

For the Low value AND CTTA option for contactless, it is possible to reset the VLP Available Funds to the VLP Funds Limit with a successful PIN verification over the contact interface. This behavior is controlled by ADA byte 3 bit 5, which if set means that the VLP Available Funds shall be reset to the VLP Funds Limit whenever the offline PIN is successfully verified, the card is not a new card, and the transaction is approved.

When Issuer Authentication is successful, the application resets the Last Successful Issuer Update ATC Register to the value of the ATC.

H.3.4 Issuer-to-Card Script Processing (Chapter 14)

When an Issuer Script command is successfully completed, the application resets the Last Successful Issuer Update ATC Register to the value of the ATC.

H.3.5 Data Dictionary (Appendix A)

New ways are added to the description in Appendix A of how to calculate the Available Offline Spending Amount data element value, depending on which low value option is supported for contactless transactions.

If the card logs qVSDC transactions in the card Transaction Log, and the application uses the ADA byte 3 bits 8-6 to control logging for contact transactions, then the application shall also use the ADA bits to control logging for qVSDC transactions.

The following data elements are added: Contactless Transaction Counter (CLTC), Contactless Transaction Counter Lower Limit (CLTCLL), Contactless Transaction Counter Upper Limit (CLTCUL), and the VLP Reset Threshold.

H.3.6 Commands for Financial Transactions (Appendix C)

If the card also supports qVSDC, then the Available Offline Spending Amount will be calculated according to the low-value option specified in the CAP.

The Cumulative Total Transaction Amount (CTTA), which may also be used by the contactless functionality, will be reset after a successful PUT DATA to the Cumulative Total Transaction Amount Limit (CTTAL) if the ‘Do not reset CTTA during GENERATE AC’ bit of the ADA is set to 1b.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

The VLP Available Funds will be reset after a successful PUT DATA to the VLP Funds Limit if the 'Do not reset VLP Available Funds during GENERATE AC' bit of the ADA is set to 1b.

A successful PUT DATA to the Application Capabilities may be used to enable or disable the contactless functionality; and also to indicate whether the functionality (if disabled) may be automatically re-enabled after an online approved transaction where issuer authenticaton requirements are met (see section 13.7), or is only allowed after a successful issuer script command.

H.3.7 Issuer Discretionary Data Options (Appendix J)

If the card also supports qVSDC functionality, then the Available Offline Spending Amount will be calculated according to the low-value option specified in the CAP.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

I Transaction Log

VIS defines optional support for a transaction log as defined in *EMV Book 3*, Annex D.

If transaction logging is supported, the SFI containing the transaction log must be in the range 11-30 ('0B' to '1E'). It is recommended that the SFI containing the transaction log be an issuer configurable value (identified at the time of personalization by the issuer in the Log Entry), but card implementations may choose to fix the SFI value(s) which are supported for transaction logging. If the card implementations supports EMV-CPS, then SFI values 13 and 14 ('0D' and '0E') are reserved for other purposes and cannot be used for transaction logging.

Byte 3 of the ADA includes three bits reserved to control logging of transactions:

- Do not include offline approved transactions in the transaction log
- Do not include online approved transactions in the transaction log
- Include declined transactions in the transaction log

Using these bits to control transaction logging is optional if the application supports transaction logging. If the ADA bits are used to control logging of transactions, the default behavior is to log all approved transactions.

If the card does not support transaction logging (or does support transaction logging but does not use ADA byte 3, bits 8-6, to determine which transactions are logged), then the application should be designed to not take any action based on the setting of these bits, regardless of the value personalized.

For personalization of cards that do not support logging or do not use the ADA bits to determine which transactions are logged, ADA byte 3, bits 8-6 should be treated as RFU and should be personalized to 000b.

Updates to the log occur:

- Just prior to card response to first GENERATE AC (if online processing was not requested) for offline approvals or offline declines according to ADA settings
- Just prior to card response to second GENERATE AC (if online processing was requested in first GENERATE AC) for online/offline approvals or declines according to ADA settings

Visa recommends only updating the transaction log for the following Transaction Types:

- '00' - Purchase
- '01' - Cash
- '11' - Quasi cash

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

On dual-interface cards, issuers may choose to limit access to the transaction log to any of the following options:

- only available over the contact interface
- only available over the contactless interface
- available over both the contact and contactless interfaces

The transaction log may only be accessed over the interface used for a transaction if the Log Format is present in the application and the Log Entry data element was returned to the device in the final SELECT response.

Implementations may support an option where log access requires successful verification of a PIN. Visa rules for PIN entry and verification apply.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

J Issuer Discretionary Data Options

This appendix describes an option that permits issuers to more closely track funds at the host, by allowing placement of specific data into the Issuer Discretionary Data portion of the Issuer Application Data (Tag '9F10').

Note: *Support for this option may be required for certain products.*

If this option is supported for VIS, this data is provided in the response to the GENERATE AC command for all types of Application Cryptogram (AAC, ARQC, and TC).

This appendix includes the following sections:

J.1 Issuer Discretionary Data Options

J.2 Personalization for IDD

J.3 Issuer Application Data Returned in GENERATE AC

J.4 MAC Calculation

J.5 Issuer Discretionary Data Example

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

J.1 Issuer Discretionary Data Options

The VLP Available Funds, Cumulative Total Transaction Amount (CTTA), Cumulative Total Transaction Amount Limit (CTTAL) and Available Offline Spending Amount data elements, and up to 15 bytes of static data are included in various options for data to be sent online in authorizations at the issuer's discretion. An issuer may elect to send any one of the options described in Table J-1. With the exception of the static data option (IDD Option '0'), the IDD Options defined in this specification include a MAC generated as described in section J.4 to ensure data integrity.

Issuer Discretionary Data (IDD), if present, shall be returned following the Visa Discretionary Data in the Issuer Application Data (Tag '9F10').

When the card application responds to the GENERATE AC command, with the IDD constructed according to this appendix, the IDD consists of a one-byte length (the IDD Length) followed by either of the following:

- a one-byte IDD Option (which includes the IDD Option ID in bits 4-1), followed by the data shown in Table J-1, or
- up to 15 bytes of static data.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table J-1: IDD Options

IDD Option	IDD Length	IDD Option ID	Remaining Contents of Issuer Discretionary Data
Issuer-defined	var. 1-15 bytes for IAD format 0/1/3 Var. 1-23 bytes for IAD format 2	'0'	• Issuer-specified constant data
VLP Available Funds	10 bytes	'1'	• Value of the 5 low-order bytes of VLP Available Funds • 4-byte MAC
Cumulative Total Transaction Amount (CTTA)	10 bytes	'2'	• Value of the 5 low-order bytes of CTTA • 4-byte MAC
VLP Available Funds and CTTA	15 bytes	'3'	• Value of the 5 low-order bytes of VLP Available Funds • Value of the 5 low-order bytes of CTTA • 4-byte MAC
CTTA and Cumulative Total Transaction Amount Limit (CTTAL)	15 bytes	'4'	• Value of the 5 low-order bytes of CTTA • Value of the 5 low-order bytes of CTTAL • 4-byte MAC
Available Offline Spending Amount (AOSA)	10 bytes	'5'	• Value of the 5 low-order bytes of Available Offline Spending Amount • 4-byte MAC

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table J-1: IDD Options

IDD Option	IDD Length	IDD Option ID	Remaining Contents of Issuer Discretionary Data
AOSA and Last Successful Issuer Update ATC Register and Issuer Script Command Counter	14	'6'	• Value of the 6-byte Available Offline Spending Amount • Value of the 2-byte Last Successful Issuer Update ATC Register if Issuer Update Processing is supported for contactless. Otherwise RFU (‘0000’) • '0' in the most significant nibble, followed by the value of the 4-bit Issuer Script Command Counter in the least significant nibble. ***Note:*** *The value in the Issuer Script Command Counter bits shall be set to the same value as in the CVR.* • 4-byte MAC

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

J.2 Personalization for IDD

The Issuer Discretionary Data (IDD) returned in the response to the GENERATE AC command varies depending on the option chosen during personalization as described in Table J-1.

The IDD Length and IDD Option ID are used to choose the type of data to be returned in the Issuer Discretionary Data field. By default, Issuer Discretionary Data will not be returned. If the issuer wants to receive Issuer Discretionary Data containing the values shown in Table J-1, the above length byte and an IDD ID byte containing the IDD Option ID in bits 4-1 should be appended to the Tag '9F10' personalization value following the Visa Discretionary Data.

For example, personalizing an IDD Length of '0A' and an IDD ID of '02' would indicate that a 10-byte IDD should be returned in the response to GENERATE AC, after the IDD Length, containing the following in the order shown:

- IDD Option = '02'
- the five low-order bytes of Cumulative Total Transaction Amount (CTTA)
- a 4 byte MAC

Note: *If a data element needed to determine a calculated value (such as the Available Offline Spending Amount) is not present, then all zeros should be sent in Issuer Application Data in place of the calculated value.*

Note: *For any IDD Option that includes the Available Offline Spending Amount, see Table A-1 for requirements on determining the value of the Available Offline Spending Amount.*

Note: *Options returning VLP Available Funds are allowed only when the dual-interface card is personalized to support VLP as a low-value option for qVSDC transactions*

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

J.3 Issuer Application Data Returned in GENERATE AC

The application uses the personalized IDDLength and IDD ID (for example, '0A02') as an indicator to activate code to supply the contents of the Issuer Discretionary Data when responding to the GENERATE AC.

For example, if the personalized IDD Length and IDD ID is '0A02', then the Issuer Application Data sent in the response to the GENERATE AC would be:

Visa Discretionary Data

Length: '06'

Value: '010A03A41000' (example)

Issuer Discretionary Data

Length: '0A'

Value: '02' (IDD ID) followed by the 5 low-order bytes of Cumulative Total Transaction Amount (CTTA), followed by the 4-byte MAC calculated as described in section J.4.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

J.4 MAC Calculation

The data to be MAC'd for IDD Option IDs '1' through '6' is the two-byte Application Transaction Counter (ATC) followed by one or two five-byte amount fields and padding, constructed as shown in Table J-2.

Table J-2: MAC Calculation

IDD Option ID	Total Length of Data Block Input to MAC Calculation	Elements Input to MAC Calculation (in order shown)	Length of Element
'1'	8 bytes	ATC	2 bytes
		VLP Available Funds	5 low-order bytes
		padding	1 byte
'2'	8 bytes	ATC	2 bytes
		Cumulative Total Transaction Amount (CTTA)	5 low-order bytes
		padding	1 byte
'3'	16 bytes	ATC	2 bytes
		VLP Available Funds	5 low-order bytes
		CTTA	5 low-order bytes
		padding	4 bytes
'4'	16 bytes	ATC	2 bytes
		CTTA	5 low-order bytes
		Cumulative Total Transaction Amount Limit (CTTAL)	5 low-order bytes
		padding	4 bytes
'5'	8 bytes	ATC	2 bytes
		Available Offline Spending Amount	5 low-order bytes
		padding	1 byte

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Table J-2: MAC Calculation

IDD Option ID	Total Length of Data Block Input to MAC Calculation	Elements Input to MAC Calculation (in order shown)	Length of Element
'6'	16 bytes	ATC	2 bytes
		IDD ID	1 byte
		Available Offline Spending Amount	6 bytes
		Last Successful Issuer Update ATC Register	2 bytes
		Issuer Script Command Counter	1 byte
		padding	4 bytes

Note: *Protection of the Issuer Discretionary Data contents for IDD Option ID '0' are beyond the scope of this specification..*

The four-byte MAC is generated as illustrated in Figure B-1, using a session key derived from the MAC UDK using the method defined in section B.4.

J.4.1 Padding for IDD MAC Generation

There are two padding methods supported for generation of the IDD MAC.

The first method is similar to the padding method used for CVN 10. This is referred to as the padding method '00', which adds as many bytes of '00' as necessary to obtain a data block with a length divisible by eight (see section D.3.2, step 3).

The second method is referred to as the padding method '80', which adds one mandatory '80' byte at the end of the data block and as many bytes of '00' as necessary to obtain a data block with a length divisible by eight. The method is identical to the padding method for Secure Messaging for Integrity and Authentication, as described in section B.2.4, step 4.

In order for the card to recognize the padding method chosen by the issuer, the Application Default Action indicates the padding method to be used when generating the MAC for inclusion in the Issuer Discretionary Data as follows:

- If the ‘Padding method '80' supported’ bit of the ADA is set to 1b, then padding method '80' shall be used.
- If the ‘Padding method '80' supported’ bit of the ADA is set to 0b, then padding method '00' shall be used.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

J.5 Issuer Discretionary Data Example

Visa Discretionary Data (Mandatory)

Length: '06'

Value: '010A03000000' (assuming CVN 10)

Issuer Discretionary Data

Length: '0A' (expected length of the concatenated data elements in the IDD in GEN AC response)

Value: '02' (IDD ID to request Cumulative Total Transaction Amount (CTTA))

The TLV personalized for the above example would be as follows:

Tag: '9F10'

Length: '09'

Value: '06010A030000000A02'

When the card responds with Issuer Application Data containing the IDD (with the CTTA value = '112233445566', and the MAC = '1A2B3C4D'), the TLV for this example would be:

Tag: '9F10'

Length: '12'

Value: '06010A030000000A0222334455661A2B3C4D'

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Glossary

This is a glossary of terms used in this specification; it is not intended as a data dictionary. For descriptions of data elements, see Appendix A-1, Data Element Descriptions.

a

alpha

AAC

Application Authentication Cryptogram

AC

Application Cryptogram

acquirer

A Visa customer that signs a merchant or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction into interchange.

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

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

an

alphanumeric

ans

alphanumeric special

ANSI

American National Standards Institute. A U.S. standards accreditation organization.

AOSA

Available Offline Spending Amount

APDU

Application Protocol Data Unit

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.

Application Cryptogram

Cryptogram returned by the ICC in the response of the GENERATE AC command; one of the following:

- TC Transaction Certificate indicates approval
- ARQC Authorization Request Cryptogram requests online processing
- AAC Application Authentication Cryptogram indicates decline

Application Elementary File

A set of data or records in a file that uses a single Short File Identifier (SFI).

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

ARPC

Authorization Response Cryptogram

ARQC

Authorization Request Cryptogram

ASCII (American Standard Code for Information Interchange)

One of multiple standards for digital encoding of text characters.

ASI

Application Selection Indicator

ATC

Application Transaction Counter

ATM

Automated Teller Machine: 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.

AUC

Application Usage Control

Auth.

authentication

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

b

binary

Bank Identification Number (BIN)

A 6-digit number assigned by Visa and used to identify a customer 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 customers.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

BIC

Bank Identifier Code

BIN

BASE Identification Number

byte

8 bits of data.

C

conditional

CA

Certificate Authority

CAM

Card Authentication Method

CAP

Card Additional Processes

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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/Credit (VSDC).

CDA

Combined DDA/Application Cryptogram Generation

CDOL

Card Risk Management Data Object List

Cert.

certificate

Certificate Authority (CA)

A trusted central administration that issues and revokes certificates.

chargeback

A transaction that an issuer returns to an acquirer.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

chip

An electronic component designed to perform processing or memory functions.

chip card

A card embedded with a chip that communicates information to a point-of-transaction terminal.

chip-capable

A card acceptance device that is designed and constructed to facilitate the addition of a chip reader/writer.

CID

Cryptogram Information Data

CLA

Class Byte of the Command Message

clearing

The collection and delivery to the issuer of a completed transaction record from an acquirer.

cleartext

See plaintext.

CLTC

Contactless Transaction Counter

CLTCLL

Contactless Transaction Counter Lower Limit

CLTCUL

Contactless Transaction Counter Upper Limit

cn

compressed numeric

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Combined Dynamic Data Authentication/Application Cryptogram Generation (CDA)

A type of Offline Data Authentication where the card combines generation of a cryptographic value (dynamic signature) for validation by the terminal with generation of the Application Cryptogram to ensure that the Application Cryptogram came from the valid card.

Cons.

consecutive

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.

CSU

Card Status Update

CTTA

Cumulative Total Transaction Amount

CTTAL

Cumulative Total Transaction Amount Limit

CTTAUL

Cumulative Total Transaction Amount Upper Limit

CTC

Consecutive Transaction Counter

CTCL

Consecutive Transaction Counter Limit

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

CTCUL

Consecutive Transaction Counter Upper Limit

CTCI

Consecutive Transaction Counter International

CTCIL

Consecutive Transaction Counter International Limit

CTCIC

Consecutive Transaction Counter International Country

CTCICL

Consecutive Transaction Counter International Country Limit

CTIUL

Consecutive Transaction International Upper Limit (upper limit used for both the Consecutive Transaction Counter International and the Consecutive Transaction Counter International Country)

Cum.

cumulative

CVM

Cardholder Verification Method

CVM List

An issuer-defined list contained within a chip application establishing the hierarchy of methods for verifying the authenticity of a cardholder.

CVN

Cryptogram Version Number

CVN 10

Refers to the cryptogram method used to generate the Application Cryptogram if the Issuer Application Data is personalized to used Cryptogram Version Number 10 ('0A').

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

CVN 12

Refers to the proprietary cryptogram method used to generate the Application Cryptogram if the Issuer Application Data is personalized to used Cryptogram Version Number 12 ('0C').

CVN 18

Refers to the cryptogram method used to generate the Application Cryptogram if the Issuer Application Data is personalized to used Cryptogram Version Number 18 ('12').

CVN 50 through CVN 59

Refers to the proprietary cryptogram method used to generate the Application Cryptogram if the Issuer Application Data is personalized to used Cryptogram Version Numbers 50 through 59 ('32' through '3B').

CVR

Card Verification Results

CVV

Card Verification Value

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.

DDA

Dynamic Data Authentication

DDF

Directory Definition File

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

DDOL

Dynamic Data Authentication Data Object List

DEA

Data Encryption Algorithm

decryption

The process of transforming ciphertext into cleartext.

DES

Data Encryption Standard

DES key

A secret parameter of the Data Encryption Standard algorithm.

DES keys by definition are of odd parity, as indicated in the Federal Information Processing Standards publication FIPS 46-3.

DF

dedicated file

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.

DKI

Derivation Key Index

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 signature using transaction-specific data elements for validation by the terminal to protect against skimming.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

EBCDIC (Extended Binary Coded Decimal Interchange Code)

One of multiple standards for digital encoding of text characters.

EEPROM

Electrically Erasable Programmable Read-Only Memory

EMV specifications (EMV)

Technical specifications developed and maintained by EMVCo to create standards and ensure global interoperability for use of chip technology in the payment industry. Note that in order to support EMV, cards and terminals must also meet the requirements described in the bulletins available on the EMVCo website.

EMVCo LLC (EMVCo)

The organization of payment systems that manages, maintains and enhances the EMV specifications. EMVCo is currently operated by Visa Inc., MasterCard Worldwide, and JCB International.

Enable

To activate (or turn on) optional functionality that is implemented in a card or application.

ENC MDK

Master Data Encipherment DEA Key

ENC UDK

Unique Data Encipherment DEA Key

encryption

The process of transforming cleartext into ciphertext.

expired card

A card on which the embossed, encoded, or printed expiration date has passed.

FCI

File Control Information

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

FCP

File Control Parameters

floor limit

A currency amount that Visa has established for single transactions at specific types of merchants, above which online authorization is required.

FMD

File Management Data

GPO

GET PROCESSING OPTIONS

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.

hex.

hexadecimal

HHMMSS

hours, minutes, seconds

host data capture system

An acquirer authorization system that retains authorized transactions for settlement without notification from the terminal that the transaction was completed.

HSM

Hardware Security Module

IA

Issuer Authentication

IAC

Issuer Action Code

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

IAD

Issuer Application Data

IAuD

Issuer Authentication Data

IBAN

International Bank Account Number

IC

integrated circuit

ICC

integrated circuit card

iCVV

Alternate CVV for use on the magnetic stripe image of the Track 2 data on the chip

IDD

Issuer Discretionary Data

IEC

International Electrotechnical Commission

IFD

interface device

IIN

Issuer Identification Number

Implement

To make a card or application capable of performing a functionality. Functionality that is implemented may also need to be enabled (for example, by personalization of specific data) before it can be used. *See* enable and support.

INS

Instruction Byte of the Command Message

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Integrated Circuit Card (ICC)

See chip card.

Integrated Circuit Chip

See chip.

interchange

The exchange of clearing records between customers.

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.

Int'l

international

ISO

International Organisation for Standardisation

issuer

A Visa customer 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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

Lc

Length of the Command Data Field

L_D

Length of the plaintext data in the Command Data Field

Le

Expected Length of the Response 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

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

MCC

Merchant Category Code

MDK

Master Derivation Key

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.

MSD (Magnetic Stripe Data)

A contactless payment transaction type defined in VCPS (and not used in VIS).

multi-application

The presence of multiple applications on a chip card (for example, payment, loyalty, and identification).

n

numeric

N/A

not applicable

N_{CA}

Length of the Certification Authority Public Key Modulus

N_I

Length of the Issuer Public Key Modulus

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

nibble

The four most significant or least significant bits of a byte of data.

N_{IC}

Length of the ICC Public Key Modulus

No.

number

O

optional

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 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 three forms: Static Data Authentication (SDA), Dynamic Data Authentication (DDA), and Combined DDA/AC Generation (CDA).

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 dynamic data authentication

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. Includes both DDA and CDA.

offline PIN

A PIN value stored on the card that is validated at the point of transaction between the card and the terminal.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

offline-capable

A card acceptance device that is able to perform offline approvals.

offline-only terminal

A card acceptance device that is not capable of sending transactions online for issuer authorization.

online authorization

A method of requesting an authorization through a communications network other than voice to an issuer or issuer representative.

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.

online-capable terminal

A card acceptance device that is able to send transactions online to the issuer for authorization.

online-only card

An online-only card is a card that does not approve transactions offline, but instead requests an online authorization. An online-only card will decline transactions offline if the transaction does not go online for authorization.

P1

Parameter 1

P2

Parameter 2

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

PAN

Primary Account Number

PDOL

Processing Options Data Object List

personalization

The process of populating a card with the application data that makes it ready for use.

PIN

Personal Identification Number

PIN-Expecting card

A card that is configured to typically perform Offline PIN at POS, and to request to go online if offline PIN is not performed or not successful on a card that supports the optional Card Risk Management check for PIN Verification Not Performed or Not Successful for a PIN-Expecting Card.

PIX

Proprietary Application Identifier Extension

PK

public key

PKI

Certificate Authority Public Key Index

plaintext

Data in its original unencrypted form.

PLUS

A global ATM network.

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

POS

point of service

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.

PSD

Profile Selection Diversifier

PSE

Payment Systems Environment

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.

PVV

PIN Verification Value

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

qVSDC

quick VSDC, a method specified in VCPS for conducting offline-capable contactless chip transactions.

R

required

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.

RFU

Reserved for Future Use

RID

Registered Application Provider Identifier

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

SAD

Signed Static Application Data

SAM

Secure Access Module

SDA

Static Data 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 allows messages to be sent from one entity to another, while protecting against unauthorized modification or viewing of the contents.

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 customer to another or to Visa, as a result of clearing.

SFI

Short File Identifier

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.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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.

Support

To use a functionality that is both implemented and enabled in the card or application.

SW1 SW2

Status Words

TAC

Terminal Action Codes

TC

Transaction Certificate

TDOL

Transaction Certificate Data Object List

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.

TLV

tag-length-value

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.

TSI

Transaction Status Information

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

TVR

Terminal Verification Results

Txn.

transaction

UDK

Unique DEA Key

VCPS

Visa Contactless Payment Specification

V.I.P. System

VisaNet Integrated Payment System, the online processing component of VisaNet.

var.

variable

VIS

Visa Integrated Circuit Card Specification

Visa Certificate Authority (CA)

A Visa-approved organization certified to issue certificates to participants in a Visa payment service.

Visa Contactless Payment Specification (VCPS)

A Visa specification defining requirements for conducting a payment transaction over a contactless interface.

Visa Low-value Payment (VLP)

A counter that may be reset over the contact interface and may be used to manage offline risk over the contactless interface.

Visa Smart Debit/Credit (VSDC)

The Visa payment service offerings for chip-based debit and credit programs. These services are supported by VisaNet processing, as well as by Visa rules and regulations; and are based on EMV and VIS, VCPS, or EMV Common Core Definitions (CCD) – including Common Payment Application (CPA) – specifications.

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

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 customers.

VLP

Visa Low-value Payment

YDDD

year, day:

- Y = right-most digit of the year (‘0’–‘9’)
- DDD = Julian day of the year (‘001’–‘366’)

YYMM

year, month:

- YY = year (‘00’–‘99’)
- MM = month (‘01’–‘12’)

YYMMDD

year, month, day:

- YY = year (‘00’–‘99’)
- MM = month (‘01’–‘12’)
- DD = day (‘01’–‘31’)

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Index

A

AAC 126, 130, 134, 158, 183, 241, 466, 470, 471, 475
AC 88, 124, 130, 139, 170, 180, 263, 419, 470, 475
Account Type 258
Acquirer Identifier 258
ADA. *See* Application Default Action
Additional Terminal Capabilities 258
ADF. *See* Application Definition File
advice message 160, 213, 225
AEF. *See* Application Elementary File
AFL. *See* Application File Locator
AID 46, 50, 274
AIP. *See* Application Interchange Profile
algorithms 463
AMD. *See* Application Management Data
Amount X and Amount Y 101
Amount, Authorized 117, 131, 138, 181, 188, 469, 474
    Amount, Authorized (Binary) 261
    Amount, Authorized (Numeric) 261
Amount, Other 181, 469, 474
    Amount, Other (Binary) 261
    Amount, Other (Numeric) 262
Amount, Reference Currency (Binary) 262
an (data element format) 253
ans (data element format) 253
AOSA. *See* Available Offline Spending Amount
Application Authentication Cryptogram. *See* AAC
APPLICATION BLOCK command 42, 241, 431
application blocking 42, 51, 54, 55, 111
Application Cryptogram. *See* AC
Application Currency Code 100, 130, 180, 263
Application Currency Exponent 264
Application Default Action 100, 130, 140, 155, 160, 180, 206, 213, 217, 265
Application Definition File 47
Application Discretionary Data 272
Application Effective Date 84, 94, 97, 273
Application Elementary Files 47, 74
Application Expiration Date 84, 94, 98, 273
Application File Locator 62, 66, 74, 87, 274
Application Identifier. *See* AID
Application Interchange Profile 62, 66, 80, 84, 85, 100, 130, 170, 180, 275, 469, 474
Application Label 47, 277, 457
Application PAN 278
Application PAN Sequence Number 84, 278

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Application Preferred Name 47, 278, 457
Application Priority Indicator 47, 48, 279, 457
Application Selection 33, 39, 45, 242
    Application Selection Indicator 50
    card data 46
    commands 51
    identifying and selecting the application 56
    processing flow 57
    terminal data 50
Application Selection Indicator 280
Application Selection Registered Proprietary Data (ASRPD) 281
Application Template 282
Application Transaction Counter. *See* ATC
APPLICATION UNBLOCK command 42, 242, 432
Application Usage Control 34, 84, 94, 96, 283
Application Version Number 95, 284
    '9F08' 94
    '9F09' 95
applications, multiple on card 46
ARPC 172, 175, 189, 193, 194, 434, 471, 476, 479, 484
ARPC Response Code 172, 175, 189, 193, 434, 471, 479
ARQC 126, 130, 134, 158, 162, 165, 170, 171, 174, 183, 466, 470, 471, 475
ASCII 479
ASI. *See* Application Selection Indicator
ATC 62, 82, 116, 118, 119, 170, 180, 190, 237, 282, 419, 424, 425, 469, 474
ATM 96
AUC. *See* Application Usage Control
authentication keys and algorithms 463
Authorization Code 284
authorization message 435, 478
Authorization Request Cryptogram. *See* ARQC
Authorization Response Code 126, 181, 188, 192, 285
Authorization Response Cryptogram. *See* ARPC
authorization response message 244, 430
Available Offline Spending Amount (AOSA) 287

B

b (data element format) 252
backup, data element 256
Bank Identifier Code (BIC) 288
binary data 479
biometrics 99
Bit Mask 288
Block Length 289

C

CAM. *See* Online Card Authentication
candidate list, building the 52, 53

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Card Action Analysis 36, 40, 91, 129, 170, 176
processing 139
terminal data 138
Card Additional Processes 290
CARD BLOCK command 42, 242, 433
card data
for Application Selection 46
for Card Action Analysis 130
for Cardholder Verification 100
for Completion 180
for Initiate Application Processing 62
for Issuer Script processing 237
for Offline Data Authentication 80
for Online Processing 170
for Processing Restrictions 94
for Read Application Data 74
for Terminal Action Analysis 122
for Terminal Risk Management 116
card declined transaction offline 159
card functional requirements 39
card reader 108
Card Risk Management 138, 165, 215
Card Risk Management checks 140
Issuer Authentication Failed (or Mandatory and Not Performed) 144
Issuer Script Processed on Last Online Transaction 145
New Card 155
Offline Dynamic Data Authentication (DDA or CDA) Failed on Last Transaction 144
Offline PIN Verification Not Performed (PIN Try Limit Exceeded) 156, 157
Online Authorization Not Completed 143
SDA Failed on Last Transaction 144
Special Transactions 157
Velocity Checking for Consecutive International Country Transactions Lower Limit 149
Velocity Checking for Consecutive International Transactions Lower Limit 147
Velocity Checking for Consecutive Transactions Lower Limit 145
Velocity Checking for Contactless Offline Transactions Lower Limit 154
Velocity Checking for Cumulative Total Transaction Amount 150
Velocity Checking for VLP Contactless Transactions Reset Threshold 154
Card Risk Management Data Object List. *See* CDOL1, CDOL2
Card Status Update 172, 189
Card Status Update. *See* CSU 292
Card Verification Results. *See* CVR
cardholder confirmation 56
Cardholder Name 297
Cardholder Name—Extended 298
cardholder selection 56

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Cardholder Verification 35, 40, 99
card data 100
commands 105
processing 106
terminal data 104
Cardholder Verification Method. *See* CVM
CDA 34, 39, 73, 77, 88, 91, 131, 165, 185, 223
DDA or CDA Failure Indicator 210, 223
Offline Dynamic Data Authentication (DDA or CDA) Failed on Last Transaction check 144
CDA, DDA or SDA, determining which Offline Data Authentication to perform 86
CDOL1 122, 131, 138, 291, 464, 470, 475
CDOL2 181, 190, 291, 464, 470, 475
Certificate Authority Public Key
Certificate Authority Public Key 302
Certificate Authority Public Key Check Sum 303
Certificate Authority Public Key Exponent 303
Certificate Authority Public Key Index 79, 81, 87, 89, 102, 304
Certificate Authority Public Key Modulus 304
Certificate Expiration Date 79
Check Type 305
Chip Condition Code 306
CID. *See* Cryptogram Information Data
clearing message 435, 478
cn (data element format) 253, 479
Combined DDA/AC Generation. *See* CDA
command formats 426
command support requirements 42
Command Template 306
commands 429
mandatory, conditional and optional 42
See also individual commands:
APPLICATION BLOCK
APPLICATION UNBLOCK
CARD BLOCK
EXTERNAL AUTHENTICATE
GENERATE APPLICATION CRYPTOGRAM
GET CHALLENGE
GET DATA
GET PROCESSING OPTIONS
INTERNAL AUTHENTICATE
PIN CHANGE/UNBLOCK
PUT DATA
READ RECORD
SELECT
UPDATE RECORD
VERIFY
Comparison Blocks 306
Comparison Value x 307

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Completion 37, 40, 81, 175, 176
card data 180
processing flow 191
terminal data 188
Completion Processing 179
conditional 253
confidentiality 232, 417, 421, 430
Consecutive Transaction Counter 132, 182, 211, 307, 516
Consecutive Transaction Counter International 132, 147, 148, 160, 182, 210, 220, 224, 227, 308, 516
Consecutive Transaction Counter International Country 132, 149, 182, 210, 224, 516
Consecutive Transaction Counter International Country Limit 132, 149, 309
Consecutive Transaction Counter International Country Limit x 312
Consecutive Transaction Counter International Limit 132, 147, 148, 309
Consecutive Transaction Counter Limit 132, 310
Consecutive Transaction Counter Limit x 314
Consecutive Transaction Counter Lower Limit 133
Consecutive Transaction Counter Upper Limit 182, 183
Consecutive Transaction Counter x 311
Consecutive Transaction International Upper Limit 182, 220, 310
Contactless Counters Data Template 315
Contactless Transaction Counter 133, 183, 210, 316, 516
Contactless Transaction Counter Lower Limit 316
Contactless Transaction Counter Upper Limit 317
Conversion Currency Code 133
counters 179, 208
Counters Data Template 318
credit risk 115
Cryptogram Information Data 63, 88, 134, 139, 158, 160, 165, 171, 183, 190, 205, 208, 213, 318
cryptogram versions 466
Cryptogram Version Number 171, 319, 465, 466
CVN 10 - 466, 470, 471, 472
CVN 12 - 466, 477
CVN 18 - 466
CVN 50 to 59 - 466, 477
CSU 43, 188, 194, 195, 196, 202, 292
CSU. *See* Card Status Update
Cumulative Total Transaction Amount 134, 184, 211, 218, 320, 516
Cumulative Total Transaction Amount Limit 134, 321
Cumulative Total Transaction Amount Upper Limit 184, 218, 322
Currency Conversion
Conversion Currency Code 183
currency conversion example 153
Currency Conversion Factor 135, 184
Currency Conversion Factor x 326
Currency Conversion Parameters 135, 327

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

CVM 99
CVM Code 101
CVM Conditions 101
CVM List 35, 84, 101, 106, 298
CVM List processing, card data 100
CVM Results 302
CVM Type 101
default CVM 35
offline CVM verification 461
CVR 62, 81, 100, 109, 111, 131, 140, 158, 170, 171, 185, 190, 203, 208, 213, 237, 293, 469

D

Data Authentication Code 327
data confidentiality 245
data element formats 252
data elements 251
data encipherment 430
Data Encipherment Session Key 235, 245, 421, 424, 443, 446
Data Encryption Standard. *See* DES
data integrity, data element 256
DDA 34, 39, 73, 77, 88, 90, 131, 185
DDA Failure Indicator 81, 135, 144
DDA or CDA Failed on Last Transaction check 140
DDA or CDA Failure Indicator 161, 210, 223
Offline Dynamic Data Authentication (DDA or CDA) Failed on Last Transaction check 144
DDA, CDA or SDA, determining which Offline Data Authentication to perform 86
DDF. *See* Directory Definition File
DDOL 81, 88, 330
Default DDOL 85, 88, 328
Dedicated File Name. *See* DF Name
default CVM 35
Default DDOL 85, 88, 328
Derivation Key Index 171, 329, 477
Derivation Key Methodology 480
DES 124, 232, 471
DES cryptogram 159
DF Name 47, 328, 457
Directory Definition File 48
Directory Definition File Name 329
Directory Discretionary Template 329
Directory File 48
Directory Selection Method 52, 57
DKI. *See* Derivation Key Index
domestic 96, 97
Dual-interface Contactless and Contact 519
dynamic data authentication 34, 88
Dynamic Data Authentication Data Object List. *See* DDOL
Dynamic Data Authentication Failure Indicator 185, 330

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Dynamic Data Authentication. *See* DDA
dynamic signature 90, 165

E

EBCDIC 479
EMV 21, 22, 27, 78
    specifications 30
ENC MDK 235, 485
ENC UDK 421, 424, 425, 485
Enciphered PIN Data 331
EXTERNAL AUTHENTICATE command 42, 172, 173, 175, 202, 210, 433

F

FCI 48, 52, 418, 457
    FCI Issuer Discretionary Data 47, 331, 457
    FCI Proprietary Template 332, 457
    FCI Template 332
File Control Information. *See* FCI
File Control Parameters. *See* FCP
File Management Data. *See* FMD
FIPS publication 29
floor limits 118
    See also Terminal Floor Limit
fraud risk 115
functions
    mandatory and optional 39
    overview 33
    See also individual functions:
        Application Selection
        Card Action Analysis
        Cardholder Verification
        Completion
        Initiate Application Processing
        Issuer-to-Card Script Processing
        Offline Data Authentication
        Online Processing
        Processing Restrictions
        Read Application Data
        Terminal Action Analysis
        Terminal Risk Management

G

GENERATE AC command 42, 89, 139, 180, 190, 435
    Card Action Analysis 139
    Completion 190
GET CHALLENGE command 42, 105, 109, 437
GET DATA command 42, 105, 108, 118, 438
    data retrievable by GET DATA command 438
GET PROCESSING OPTIONS command 42, 65, 440
Go Online on Next Transaction From Previous Online Response check 142
Go Online on Next Transaction Indicator 210

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

GPO. *See* GET PROCESSING OPTIONS command

H

hash 80, 87, 89
host security module 79, 482, 485

I

IACs 84, 122, 125
    Issuer Action Code—Default 339
    Issuer Action Code—Denial 339
    Issuer Action Code—Online 339
IAuD. *See* Issuer Authentication Data
ICC Dynamic Data 81, 90, 165, 333
ICC Dynamic Number 82, 333
ICC key data 78, 80, 485
ICC PIN Encipherment PK Certificate. *See* ICC PIN Encipherment Public Key Certificate
ICC PIN Encipherment Private Key 102, 334
ICC PIN Encipherment Public Key Certificate 102, 334, 485
ICC PIN Encipherment Public Key Exponent 102, 335
ICC PIN Encipherment Public Key Remainder 102, 335
ICC PK Certificate. *See* ICC Public Key Certificate 82
ICC Private Key 80, 82, 88, 102, 165, 336
ICC Public Key 34, 80, 89
ICC Public Key Certificate 82, 89, 102, 123, 336, 485
ICC Public Key Exponent 82, 102, 337
ICC Public Key Remainder 83, 337
IDD Options 529
identifying and selecting the application 56
impact summary 27
indicators 179, 208
Initiate Application Processing 33, 39, 61
    card data 62
    processing 65
    processing flow 69
    terminal data 64
Interface Device (IFD) Serial Number 337
Interlink 46, 47
INTERNAL AUTHENTICATE command 42, 88, 90, 442
international 96, 97
International Bank Account Number (IBAN) 338
International Counters Data Template 338
ISO documents 29
Issuer Action Code. *See* IAC
Issuer Application
    Issuer Application Data 190
Issuer Application Data 131, 171, 185, 340, 435, 474
Issuer Application Data. *See* IAD
issuer approval 202, 206

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Issuer Authentication 37, 81, 155, 169, 175, 179, 203, 206, 208, 245, 417
Issuer Authentication Data 172, 189, 342, 471, 479
Issuer Authentication Failed (or Mandatory and Not Performed) on Last Transaction check 140, 144
Issuer Authentication Failure Indicator 135, 144, 171, 176, 185, 193, 194, 209, 343, 345
Issuer Authentication Indicator 135, 144, 185, 206, 344
Issuer Authentication Was Performed Using EXTERNAL AUTHENTICATE Command Indicator 171, 185
Issuer Code Table Index 47, 48, 345, 457
Issuer Country Code 346
'5F28' 84, 94
'9F57' 135, 185
Issuer Country Code (alpha2) 347
Issuer Country Code (alpha3) 347
issuer data elements
Authorization Code 284
Authorization Response Code 285
Issuer Authentication Data 342
Issuer Script Command 351
Issuer Script Identifier 353
Issuer Script Template 1 355
Issuer Script Template 2 355
issuer decline 202
Issuer Discretionary Data 171
Issuer Discretionary Data Identifier (IDD ID) 348
options 527
issuer host 169
Issuer Identification Number (IIN) 350
issuer key data 78
Issuer Private Key 82
Issuer Public Key 34, 87, 89, 102
Issuer Public Key Certificate 78, 83, 102, 350
Issuer Public Key Exponent 83, 102, 350
Issuer Public Key Remainder 83, 103, 351
Issuer Script 475
Issuer Script Command 240, 241, 351, 429
See also individual commands:
APPLICATION BLOCK
APPLICATION UNBLOCK
CARD BLOCK
PIN CHANGE/UNBLOCK
PUT DATA
UPDATE RECORD

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Issuer Script processing 37, 41, 417, 430, 471
card data 237
in authorization response 240, 244
Issuer Script Command Counter 136, 186, 210, 238, 352
Issuer Script Failure Indicator 136, 145, 186, 210, 238, 353
Issuer Script Identifier 240, 353
Issuer Script Processed on Last Online Transaction check 141
Issuer Script Results 239, 354
Issuer Script Template 240
Issuer Script Template 1 355
Issuer Script Template 2 355
key management 232
processing flow 244, 248
terminal data 239
Issuer Update 255
Issuer URL 356
Issuer-to-Card Script Processing. *See* Issuer Script processing

K

key derivation 232
keys 463
keys and certificates
Offline Data Authentication 78

L

Language Preference 47, 356, 457
Last Online ATC Register 116, 118, 119, 136, 155, 186, 211, 357
Last Successful Issuer Update ATC Register 193, 194, 357
List of AIDs Method 52, 54, 58
List of supported applications 50
Log Entry 358
Log Format 358
logging. *See* transaction log
Lower Consecutive Offline Limit 359
'9F14' 116, 119
'9F58' 132

M

MAC 232, 238, 245, 417, 418, 430, 443
MAC Calculation 533
MAC MDK 232, 485
MAC Session Key 232, 245, 418, 424
MAC UDK 232, 418, 424, 425
Unique MAC DEA Key A 402
Unique MAC DEA Key B 403
mandatory 22
Master Data Encipherment DEA Key. *See* ENC MDK
Master Derivation Key. *See* MDK
Master Message Authentication Code DEA Key. *See* MAC MDK
Maximum Target Percentage to be Used for Biased Random Selection 117, 359

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

may 22
MDK 484
Merchant Category Code 359
Merchant Forced Transaction Online 118
Merchant Identifier 360
Merchant Name and Location 360
Message Authentication Code. *See* MAC
message integrity 232, 245, 417, 418
must 22

N

n (data element format) 253
Negative Action 361
new card 118, 119, 217, 439
New Card check 141, 155
Number of Blocks 362

O

offline approval 121, 158, 162, 190
offline CVM verification 461
Offline Data Authentication 34, 39, 77, 87, 123
    determining whether to perform SDA, DDA or CDA 86
    keys and certificates 78
    SDA 87
offline data authentication
    terminal data 85
offline decline 121, 158, 190
    Offline Decline Requested by Card Indicator 136, 216, 223, 363
offline dynamic data authentication 34
Offline Enciphered PIN 80, 99, 104, 105, 109, 437
Offline PIN 156, 217
Offline PIN Verification Not Performed (PIN Try Limit Exceeded) check 142, 156, 157
Offline Plaintext PIN 99, 105, 109
online authorization 121, 158, 162, 190, 192
    Online Authorization Indicator 136, 143, 162, 186, 210, 364
    Online Authorization Not Completed (on previous transaction) check 140, 143
Online Card Authentication 36, 169
online PIN 99
Online Processing 36, 40, 91, 169, 179
    card data 170
    flow 177
    online response data 172
    processing 173
    terminal data 172
Online Processing Requested, Online Authorization Not Completed 215
online request 171, 174
Online Requested by Card Indicator 136, 143, 145, 150, 152, 156, 365
online response 174
Online Response Data, Online Processing 172

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

optional 22, 253

P

PAN 84, 116, 118, 232, 481
PAN Sequence Number 232, 481
partial name selection 54
Payment Account Reference (PAR) 366
Payment Systems Directory 48, 53
Payment Systems Environment 48, 51, 52, 242
PDOL 47, 48, 51, 64, 369, 457
personalization 429, 485
PIN 232
    cardholder-selected 246
    changing 243, 443
    encipherment 109, 232
    unblocking 243, 443
PIN block generation, input data 444
PIN CHANGE/UNBLOCK command 42, 103, 243, 246, 443
PIN pad 108
PIN Pad Secret Key 366
PIN Try Counter 103, 105, 108, 110, 111, 136, 156, 186, 243, 367, 439
PIN Try Limit 103, 105, 110, 111, 156, 160, 186, 217, 243, 367
PIN Try Limit Exceeded (Offline PIN Verification Not Performed) check 217
PIN Verification Value. *See* PVV
PIX 46, 50, 379
PLUS 46, 47
Position in Profile Selection Input Data 368
Positive Action 368
post-issuance updates 141, 169
Processing Options Data Object List. *See* PDOL
processing overview 33
Processing Restrictions 34, 39, 93
    card data 94
    processing 95
        Application Effective Date 97
        Application Expiration Date 98
        Application Usage Control 96
        Application Version Number 95
    terminal data 95
Profile Behavior 67, 68, 502
Profile Behavior -- Default 507
Profile Behavior -- Minimum Functionality 508
Profile Control 136, 186, 370
Profile ID 137, 187, 361, 368, 376

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Profile Selection 66, 67, 378, 488, 499
Bit Mask 288
Block Length 289
Check Type 305, 377, 495
Comparison Blocks 306
Comparison Value x 307
Negative Action 361, 377
Number of Blocks 362
Position in Profile Selection Input Data 368
Positive Action 368, 377
Profile ID 361, 368, 376
Profile Selection Entry x 377
Profile Selection File 377
Profile Selection Diversifier 376, 378, 488, 489
Profile Selection Entry 288, 289, 305, 306, 307, 331, 361, 362, 368, 377, 378, 495
Profile Selection File 377
Profile Selection File Entry 276, 378
Proprietary Application Identifier Extension. *See* PIX
Proprietary Authentication Data 379
PSD. *See* Profile Selection Diversifier
PUT DATA command 42, 243, 451
PVV 243, 246

R

random transaction selection 118
Read Application Data 33, 39, 73
card data 74
processing 75
terminal data 75
READ RECORD command 42, 51, 52, 74, 75, 456
Receive GENERATE AC command, completion of 192, 202
recommended 22
Reference PIN 103, 105, 110, 243, 380, 419, 443, 485
references 28
EMV specifications 30
FIPS publication 29
ISO documents 29
Visa documents 30
referral 202, 206
Registered Application Provider Identifier. *See* RID
required 22, 253
Response Message Template Format 1 381
Response Message Template Format 2 381
retrieval capability, data element 255
RFU 23
RID 46, 50, 83, 87, 89, 104, 380
RSA 78

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

S

SAD. *See* Signed Static Application Data
SDA 34, 39, 73, 77, 87, 131
SDA Failed on Last Transaction check 140, 144
SDA Failure Indicator 85, 137, 144, 160, 187, 210, 223, 383
SDA Tag List 85, 87, 383
SDA, DDA or CDA, determining which Offline Data Authentication to perform 86
secret data elements 257
secure messaging 232, 238, 244, 417, 430
SELECT command 42, 51, 56, 242, 457
Service Code 381
session key generation 424
SFI. *See* Short File Identifier
shall 22
Short File Identifier 48, 51, 74, 243, 382, 457
should 22
signature, cardholder 99
Signed Dynamic Application Data 83, 88, 90, 165, 382
Signed Static Application Data 84, 87, 123, 382, 485
skimming 77
special device 242, 255, 438
special transactions 157
Static Data Authentication. *See* SDA
stolen cards 99, 242

T

TACs 124, 125
Terminal Action Code—Default 384
Terminal Action Code—Denial 384
Terminal Action Code—Online 384
Target Percentage to be Used for Random Selection 117, 383
TC 127, 130, 134, 158, 162, 165, 183, 206, 208, 223, 466, 470, 475
Terminal Action Analysis 35, 40, 121
card data 122
processing 125
terminal data 124
Terminal Capabilities 385
Terminal Country Code 95, 131, 138, 181, 189, 386, 469, 474

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

terminal data
for Application Selection 50
for Card Action Analysis 138
for Cardholder Verification 104
for Initiate Application Processing 64
for Issuer Script processing 239
for offline data authentication 85
for Online Processing, Issuer Authentication 172
for Processing Restrictions 95
for Read Application Data 75
for Terminal Action Analysis 124
for Terminal Risk Management 117

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

terminal data elements
Account Type 258
Acquirer Identifier 258
Additional Terminal Capabilities 258
Amount, Authorized (Binary) 261
Amount, Authorized (Numeric) 261
Amount, Other (Binary) 261
Amount, Other (Numeric) 262
Amount, Reference Currency (Binary) 262
Application Identifier (AID) 275
Application Selection Indicator 280
Application Version Number 284
Authorization Response Code 285
Cardholder Verification Method (CVM) Results 302
Certificate Authority Public Key 302
Certificate Authority Public Key Check Sum 303
Certificate Authority Public Key Exponent 303
Certificate Authority Public Key Index (PKI) 304
Certificate Authority Public Key Modulus 304
Chip Condition Code 306
Command Template 306
Default Dynamic Data Authentication Data Object List (Default DDOL) 328
Enciphered Personal Identification Number (PIN) Data 331
Interface Device (IFD) Serial Number 337
Issuer Script Results 354
Maximum Target Percentage to be Used for Biased Random Selection 359
Merchant Category Code 359
Merchant Identifier 360
Merchant Name and Location 360
Personal Identification Number (PIN) Pad Secret Key 366
Proprietary Application Identifier Extensions (PIX) 379
Registered Application Provider Identifier (RID) 380
Target Percentage to be Used for Random Selection 383
Terminal Action Code—Default 384
Terminal Action Code—Denial 384
Terminal Action Code—Online 384
Terminal Capabilities 385
Terminal Country Code 386
Terminal Floor Limit 386
Terminal Identification 386
Terminal Risk Management Data 387
Terminal Type 387
Terminal Verification Results (TVR) 389
Threshold Value for Biased Random Selection 391
Transaction Amount 393
Transaction Certificate (TC) Hash Value 394
Transaction Currency Code 394
Transaction Currency Exponent 395

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Transaction Date 395
Transaction Personal Identification Number (PIN) Data 395
Transaction Reference Currency Code 396
Transaction Reference Currency Conversion 396
Transaction Reference Currency Exponent 397
Transaction Sequence Counter 397
Transaction Status Information (TSI) 398
Transaction Time 398
Transaction Type 399
Unpredictable Number 403
Terminal Floor Limit 117, 386
Terminal Identification 386
Terminal Risk Management 35, 40, 115, 125
card data 116
processing 118
terminal data 117
Terminal Risk Management Data 387
Terminal Type 387
terminal velocity checking. *See* velocity checking, terminal
Terminal Verification Results. *See* TVR
terminated transactions 23
terminology
may 22
recommended 22
shall 22
should 22
conditional 253
mandatory 22
optional 22, 253
required 22, 253
Threshold Value for Biased Random Selection 117, 391
Track 1 Discretionary Data 246, 392
Track 2 Discretionary Data 392
Track 2 Equivalent Data 246, 393
Transaction Amount 393
transaction authorized online, Completion 192
Transaction Certificate. *See* TC
Transaction Currency Code 131, 138, 181, 189, 394, 469, 474
Transaction Currency Exponent 395
Transaction Date 95, 98, 181, 395, 469, 474
transaction flow, sample 38
transaction log 525
Log Entry 358
Log Format 358
transaction log (in terminal) 117
Transaction PIN 103, 104, 105, 109
Transaction PIN Data 395

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Transaction Reference Currency
Transaction Reference Currency Code 396
Transaction Reference Currency Conversion 396
Transaction Reference Currency Exponent 397
Transaction Sequence Counter 397
Transaction Status Information 117, 239, 398
Transaction Time 398
Transaction Type 95, 181, 399, 469, 474
TSI. *See* Transaction Status Information
TVR 117, 122, 131, 138, 181, 189, 239, 389, 469, 474

U

UDKs 171, 175, 193, 472, 481, 484, 485
Unique DEA Key A 401
Unique DEA Key B 401
unable to go online 192, 215, 223
Unique Data Encipherment DEA Key. *See* ENC UDK
Unique Data Encipherment DEA Keys
Unique Data Encipherment DEA Key A 399
Unique Data Encipherment DEA Key B 400
Unique DEA Key. *See* UDK
Unique Message Authentication Code DEA Key. *See* MAC UDK
Unpredictable Number 81, 85, 181, 403, 469, 474
update capability, data element 253
UPDATE RECORD command 43, 243, 246, 458
Upper Consecutive Offline Limit 404
'9F23' 116, 119

V

VCPS. See *Visa Contactless Payment Specification* 30
velocity checking, card 129
during Card Action Analysis
Velocity Checking for Consecutive International Country Transactions Lower Limit check 141, 149
Velocity Checking for Consecutive International Transactions Lower Limit check 141, 147
Velocity Checking for Consecutive Transactions Lower Limit check 145
Velocity Checking for Contactless Offline Transactions Lower Limit check 141
Velocity Checking for Cumulative Total Transaction Amount Lower Limit check 141, 150
Velocity Checking for Total Consecutive Transactions Lower Limit check 141
Velocity Checking for VLP Contactless Offline Transactions Lower Limit check 154
Velocity Checking for VLP Contactless Transactions Reset Threshold check 141, 154
during Completion
Velocity Checking for Consecutive International Country Transactions Upper Limit check 221
Velocity Checking for Consecutive International Transactions Upper Limit check 219
Velocity Checking for Consecutive Transactions Upper Limit check 216
Velocity Checking for Cumulative Total Transaction Amount Upper Limit check 218
velocity checking, terminal 118, 119, 439
VERIFY command 43, 103, 105, 109, 156, 461
Visa Certificate Authority 78
Visa Certificate Authority User's Guide 79
Visa Contactless Payment Specification 30

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.

Visa discretionary data 404, 435
Visa documents 30
Visa Electron 46, 47
Visa Integrated Circuit Card Specification
    impact summary 27
    revisions 27
Visa Integrated Circuit Card Specification Application Overview 30
Visa Private Key 78, 102
Visa Public Key 78, 87
Visa Transaction Acceptance Device Guide 24, 30, 124
Visa Transaction Acceptance Device Requirements 24, 30, 124, 384
VisaNet 469, 474
VLP
    VLP Available Funds 405
    VLP Funds Limit 405
    VLP Reset Threshold 406
    VLP Single Transaction Limit 406
VLP Available Funds 516
VSDC Member Implementation Guide for Acquirers 31
VSDC Personalization Specification 241, 242
VSDC Personalization Specification 30

Y

Y1 Authorization Response Code 127
Y3 Authorization Response Code 188, 192, 215, 223

Z

Z1 Authorization Response Code 126
Z3 Authorization Response Code 127, 188, 192, 215, 223

Portions © 1998–2007 Visa International Service Association and © 2008 Visa Inc. © 2009 Visa Inc. © 2016 Visa Inc. All Rights Reserved. This Specification is proprietary and confidential to Visa International Service Association and Visa Inc.