GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform Card Specification

Version 2.2.1

Public Release

January 2011

Document Reference: GPC_SPE_034



Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights or other intellectual property rights of which they may be aware which might be infringed by the implementation of the specification set forth in this document, and to provide supporting documentation. The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited . GlobalPlatform is a Trademark of GlobalPlatform, Inc.

Petitioner Samsung Ex-1006, 0001

This page intentionally left blank.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0002

Table of Contents

1 INTRODUCTION 2

1.1 Audience 3

1.2 IPR Disclaimer 3

1.3 Normative References 3

1.4 Terminology and Definitions 5

1.5 Abbreviations and Notations 8

1.6 Revisions History 10
1.6.1 Open Platform Card Specification v2.0 to Open Platform Card Specification v2.0.1 10
1.6.2 Major Adjustments in GlobalPlatform Card Specification v2.1 10
1.6.3 Revisions in GlobalPlatform Card Specification v2.1.1 12
1.6.4 Major Adjustments in GlobalPlatform Card Specification v2.2 13
1.6.5 Minor Adjustments in GlobalPlatform Card Specification v2.2.1 16

2 SYSTEM ARCHITECTURE 18

3 CARD ARCHITECTURE 19

3.1 Security Domains 20

3.2 Global Services Applications 20

3.3 Runtime Environment 20

3.4 Trusted Framework 20

3.5 GlobalPlatform Environment (OPEN) 21

3.6 GlobalPlatform API 21

3.7 Card Content 21

3.8 Card Manager 22

4 SECURITY ARCHITECTURE 23

4.1 Goals 23

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0003

4.2 Security Responsibilities and Requirements 23
4.2.1 Card Issuer's Security Responsibilities 23
4.2.2 Application Provider's Security Responsibilities 24
4.2.3 Controlling Authority's Security Responsibilities 24
4.2.4 On-Card Components' Security Requirements 24
4.2.5 Back-End System Security Requirements 26

4.3 Cryptographic support 26
4.3.1 Secure Card Content Management 27
4.3.2 Secure Communication 28

5 LIFE CYCLE MODELS 30

5.1 Card Life Cycle 30
5.1.1 Card Life Cycle States 30
5.1.2 Card Life Cycle State Transitions 32

5.2 Executable Load File/ Executable Module Life Cycle 34
5.2.1 Executable Load File Life Cycle 34
5.2.2 Executable Module Life Cycle 34

5.3 Application and Security Domain Life Cycle 34
5.3.1 Application Life Cycle States 35
5.3.2 Security Domain Life Cycle States 37

5.4 Sample Life Cycle Illustration 40

6 GLOBALPLATFORM ENVIRONMENT (OPEN) 42

6.1 Overview 42

6.2 OPEN Services 43

6.3 Command Dispatch 44

6.4 Logical Channels and Application Selection 44
6.4.1 Implicit Selection Assignment 44
6.4.2 Basic Logical Channel 45
6.4.3 Supplementary Logical Channel 48

6.5 GlobalPlatform Registry 51
6.5.1 Application/Executable Load File/Executable Module Data Elements 51
6.5.2 Card-Wide Data 53

6.6 Privileges 53
6.6.1 Privilege Definition 53
6.6.2 Privilege Assignment 54

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0004

6.6.3 Privilege Management 56

6.7 The GlobalPlatform Trusted Framework 57

7 SECURITY DOMAINS 59

7.1 General Description 59
7.1.1 Issuer Security Domain 59

7.2 Security Domain Association 60

7.3 Security Domain Services 61
7.3.1 Application Access to Security Domain Services 61
7.3.2 Security Domain Access to Applications 62
7.3.3 Personalization Support 62
7.3.4 Runtime Messaging Support 63

7.4 Security Domain Data 64
7.4.1 Issuer Security Domain 64
7.4.2 Supplementary Security Domains 65

7.5 Security Domain Keys 66
7.5.1 Key Information 66
7.5.2 Key Access Conditions 67

7.6 Data and Key Management 68

8 GLOBAL PLATFORM SERVICES 69

8.1 Global Services Applications 69
8.1.1 Registering Global Services 69
8.1.2 Application Access to Global Services 70
8.1.3 Global Service Parameters 70

8.2 CVM Application 71
8.2.1 Application Access to CVM Services 71
8.2.2 CVM Management 72

9 CARD AND APPLICATION MANAGEMENT 75

9.1 Card Content Management 75
9.1.1 Overview 75
9.1.2 OPEN Requirements 75
9.1.3 Security Domain Requirements 75

9.2 Authorizing and Controlling Card Content 77
9.2.1 DAP Verification 77

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0005

9.2.2 Load File Data Block Hash....78
9.2.3 Tokens....78

9.3 Card Content Loading, Installation and Make Selectable....78
9.3.1 Overview....78
9.3.2 Card Content Loading....79
9.3.3 Card Content Installation....80
9.3.4 Card Content Combined Loading, Installation and Make Selectable....80
9.3.5 Card Content Loading Process....81
9.3.6 Card Content Installation Process....83
9.3.7 Card Content Make Selectable Process....85
9.3.8 Card Content Combined Loading, Installation and Make Selectable Process....86
9.3.9 Examples of Loading and Installation Flow....90

9.4 Content Extradition and Registry Update....93
9.4.1 Content Extradition....93
9.4.2 Registry Update....96

9.5 Content Removal....98
9.5.1 Application Removal....100
9.5.2 Executable Load File Removal....102
9.5.3 Executable Load File and related Application Removal....103

9.6 Security Management....105
9.6.1 Life Cycle Management....105
9.6.2 Application Locking and Unlocking....106
9.6.3 Card Locking and Unlocking....107
9.6.4 Card Termination....108
9.6.5 Application Status Interrogation....109
9.6.6 Card Status Interrogation....109
9.6.7 Operational Velocity Checking....109
9.6.8 Tracing and Event Logging....110

9.7 Memory Resource Management....110

10 SECURE COMMUNICATION....112

10.1 Secure Channel....112

10.2 Explicit / Implicit Secure Channel....112
10.2.1 Explicit Secure Channel Initiation....112
10.2.2 Implicit Secure Channel Initiation....113
10.2.3 Secure Channel Termination....113

10.3 Direct / Indirect Handling of a Secure Channel Protocol....113

10.4 Entity Authentication....114

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0006

10.4.1 Authentication with Symmetric Cryptography 114
10.4.2 Authentication with Asymmetric Cryptography 114

10.5 Secure Messaging 114

10.6 Security Levels 115

10.7 Secure Channel Protocol Identifier 115

11 APDU COMMAND REFERENCE 118

11.1 General Coding Rules 120
11.1.1 Life Cycle State Coding 120
11.1.2 Privileges Coding 121
11.1.3 General Error Conditions 121
11.1.4 Class Byte Coding 122
11.1.5 APDU Message and Data Length 123
11.1.6 Confirmations in Response Messages 124
11.1.7 Implicit Selection Parameter Coding 124
11.1.8 Key Type Coding 125
11.1.9 Key Usage Qualifier Coding 125
11.1.10 Key Access Coding 126
11.1.11 Tag Coding 127
11.1.12 Data Grouping Identifier (DGI) Coding 127

11.2 DELETE Command 128
11.2.1 Definition and Scope 128
11.2.2 Command Message 128
11.2.3 Response Message 130

11.3 GET DATA Command 131
11.3.1 Definition and Scope 131
11.3.2 Command Message 131
11.3.3 Response Message 132

11.4 GET STATUS Command 135
11.4.1 Definition and Scope 135
11.4.2 Command Message 135
11.4.3 Response Message 137

11.5 INSTALL Command 140
11.5.1 Definition and Scope 140
11.5.2 Command Message 140
11.5.3 Response Message 149

11.6 LOAD Command 151
11.6.1 Definition and Scope 151

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0007

11.6.2 Command Message 151
11.6.3 Response Message 152

11.7 MANAGE CHANNEL Command 154
11.7.1 Definition and Scope 154
11.7.2 Command Message 154
11.7.3 Response Message 155

11.8 PUT KEY Command 156
11.8.1 Definition and Scope 156
11.8.2 Command Message 156
11.8.3 Response Message 159

11.9 SELECT Command 161
11.9.1 Definition and Scope 161
11.9.2 Command Message 161
11.9.3 Response Message 162

11.10 SET STATUS Command 163
11.10.1 Definition and Scope 163
11.10.2 Command Message 163
11.10.3 Response Message 164

11.11 STORE DATA Command 165
11.11.1 Definition and Scope 165
11.11.2 Command Message 165
11.11.3 Response Message 168

A GLOBALPLATFORM API 170

A.1 GlobalPlatform on a Java Card 170

A.2 GlobalPlatform on MULTOS™ 173

B ALGORITHMS (CRYPTOGRAPHIC AND HASHING) 174

B.1 Data Encryption Standard (DES) 174
B.1.1 Encryption/Decryption 174
B.1.2 MACing 174

B.2 Hashing Algorithms 174
B.2.1 Secure Hash Algorithm (SHA-1) 175
B.2.2 MULTOS Asymmetric Hash Algorithm 175

B.3 Public Key Cryptography Scheme 1 (PKCS#1) 175

B.4 DES Padding 175

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0008

B.5 Key Check Values 175

C SECURE CONTENT MANAGEMENT 176

C.1 Keys 176
C.1.1 Token and Receipt Keys 176
C.1.2 DAP Verification Keys 176

C.2 Load File Data Block Hash 177

C.3 Load File Data Block Signature (DAP Verification) 177

C.4 Tokens 178
C.4.1 Load Token 178
C.4.2 Install Token 179
C.4.3 Make Selectable Token 180
C.4.4 Extradition Token 182
C.4.5 Registry Update Token 183
C.4.6 Delete Token 184
C.4.7 Load, Install and Make Selectable Token 185

C.5 Receipts 186
C.5.1 Load Receipt 187
C.5.2 Install Receipt and Make Selectable Receipt 187
C.5.3 Extradition Receipt 188
C.5.4 Registry Update Receipt 189
C.5.5 Delete Receipt 190
C.5.6 Combined Load, Install and Make Selectable Receipt 190

C.6 DAP Verification 191
C.6.1 PKC Scheme 191
C.6.2 DES Scheme 191

C.7 GlobalPlatform on MULTOS 192
C.7.1 Keys 192
C.7.2 Cryptographic Structures 192

D SECURE CHANNEL PROTOCOL '01' (DEPRECATED) 193

D.1 Secure Communication 193
D.1.1 SCP01 Secure Channel 193
D.1.2 Mutual Authentication 193
D.1.3 Message Integrity 196
D.1.4 Message Data Confidentiality 196
D.1.5 ICV Encryption 196
D.1.6 Security Level 196
D.1.7 Protocol Rules 196

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0009

D.2 Cryptographic Keys 197

D.3 Cryptographic Usage 198
D.3.1 DES Session Keys 198
D.3.2 Authentication Cryptograms 200
D.3.3 APDU Command MAC Generation and Verification 200
D.3.4 APDU Data Field Encryption and Decryption 202
D.3.5 Key Sensitive Data Encryption and Decryption 203

D.4 Secure Channel APDU Commands 203
D.4.1 INITIALIZE UPDATE Command 205
D.4.2 EXTERNAL AUTHENTICATE Command 207

E SECURE CHANNEL PROTOCOL '02' 209

E.1 Secure Communication 209
E.1.1 SCP02 Secure Channel 209
E.1.2 Entity Authentication 210
E.1.3 Message Integrity 212
E.1.4 Message Data Confidentiality 212
E.1.5 Security Level 213
E.1.6 Protocol Rules 213

E.2 Cryptographic Keys 215

E.3 Cryptographic Algorithms 216
E.3.1 Cipher Block Chaining (CBC) 216
E.3.2 Message Integrity ICV using Explicit Secure Channel Initiation 216
E.3.3 Message Integrity ICV using Implicit Secure Channel Initiation 216
E.3.4 ICV Encryption 217

E.4 Cryptographic Usage 217
E.4.1 DES Session Keys 217
E.4.2 Authentication Cryptograms in Explicit Secure Channel Initiation 218
E.4.3 Authentication Cryptogram in Implicit Secure Channel Initiation 219
E.4.4 APDU Command C-MAC Generation and Verification 219
E.4.5 APDU Response R-MAC Generation and Verification 221
E.4.6 APDU Command Data Field Encryption and Decryption 222
E.4.7 Sensitive Data Encryption and Decryption 223

E.5 Secure Channel APDU Commands 224
E.5.1 INITIALIZE UPDATE Command 226
E.5.2 EXTERNAL AUTHENTICATE Command 228
E.5.3 BEGIN R-MAC SESSION Command 230
E.5.4 END R-MAC SESSION Command 232

F SECURE CHANNEL PROTOCOL '10' 234

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0010

F.1 Secure Communication 234
F.1.1 SCP10 Secure Channel 234
F.1.2 Initiating a Secure Channel 234
F.1.3 Certificate Verification 236
F.1.4 Entity Authentication 246
F.1.5 Session Key and Security Level Establishment 251
F.1.6 Protocol Rules 252

F.2 Cryptographic Algorithms 253
F.2.1 Asymmetric cryptography 253
F.2.2 Digest Algorithm 254
F.2.3 Message Integrity ICV 254
F.2.4 Message Integrity C-MAC and R-MAC 254
F.2.5 APDU Encryption and Decryption for Message Confidentiality 255

F.3 Cryptographic Usage 255
F.3.1 DES Session Keys 255
F.3.2 Secure Messaging 256

F.4 Commands 264
F.4.1 EXTERNAL AUTHENTICATE Command 266
F.4.2 GET CHALLENGE Command 268
F.4.3 GET DATA [certificate] Command 269
F.4.4 INTERNAL AUTHENTICATE Command 271
F.4.5 MANAGE SECURITY ENVIRONMENT Command 273
F.4.6 PERFORM SECURITY OPERATION [decipher] Command 275
F.4.7 PERFORM SECURITY OPERATION [verify certificate] Command 277

G TRUSTED FRAMEWORK INTER-APPLICATION COMMUNICATION 279

H GLOBALPLATFORM DATA VALUES AND CARD RECOGNITION DATA 280

H.1 Data Values 280

H.2 Structure of Card Recognition Data 280

H.3 Security Domain Management Data 282

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0011

Table of Figures and Tables

Figure 2-1: GlobalPlatform Architecture....18
Figure 3-1: GlobalPlatform Card Architecture....19
Figure 3-2 Card Content Relationships....22
Figure 5-1: Card Life Cycle State Transitions....33
Figure 5-2: Application Life Cycle State Transitions....37
Figure 5-3: Security Domain Life Cycle State Transitions....39
Figure 5-4: Sample Card Life Cycle and Application Life Cycles....41
Figure 6-1: GlobalPlatform Trusted Framework Roles....58
Figure 7-1: Example of Security Domain Hierarchies....60
Figure 7-2: Application Personalization through Associated Security Domain....63
Figure 7-3: Runtime Messaging Flow....64
Figure 9-1: Loading and Installation Process....79
Figure 9-2: Load and Installation Flow Diagram....91
Figure 9-3: Load Flow Diagram....92
Figure 9-4: Install Flow Diagram....93
Figure 9-5: Delegated Extradition Flow....96
Figure 9-6: Content Deletion Flow....100
Figure 9-7: Life Cycle Management Flow....106
Figure C-1: Load File Data Block Hash Calculation....177
Figure C-2: Load File Data Block Signature Calculation....178
Figure C-3 Load Token Calculation....178
Figure C-4: Install Token Calculation....179
Figure C-5: Make Selectable Token Calculation....181
Figure C-6: Extradition Token Calculation....182
Figure C-7: Registry Update Token Calculation....183
Figure C-8: Delete Token Calculation....184
Figure C-9: Load, Install and Make Selectable Token Calculation....185
Figure C-10: Load Receipt Calculation....187
Figure C-11: Install/Make Selectable Receipt Calculation....188
Figure C-12: Extradition Receipt Calculation....188
Figure C-13: Registry Update Receipt Calculation....189

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0012

Figure C-14: Delete Receipt Calculation 190
Figure C-15: Load, Install and Make Selectable Receipt Calculation 191
Figure D-1: Mutual Authentication Flow (Security Domain) 195
Figure D-2: Mutual Authentication Flow (using services of Security Domain) 195
Figure D-3: Session Key - Step 1 - Generate Derivation data 199
Figure D-4: Session Key - Step 2 - Create S-ENC Session Key 199
Figure D-5: Session Key – Step 3 - Create S-MAC Session Key 199
Figure D-6: APDU Command MAC Generation and Verification 201
Figure D-7: APDU Data Field Encryption 202
Figure E-1: Explicit Secure Channel Initiation Flow 211
Figure E-2: Create Secure Channel Session Key from the Base Key 218
Figure E-3: C-MAC Generation on Unmodified APDU 220
Figure E-4: C-MAC Generation on Modified APDU 220
Figure E-5: R-MAC Generation 222
Figure E-6: APDU Command Data Field Encryption 223
Figure F-1 - Certificate Chains - Example a 237
Figure F-2 - Certificate Chains - Example b 238
Figure F-3 Certificate Chains - Example c 238
Figure F-4 - Certificate Verification Flow 239
Figure F-5: Certificate Formation - Self Descriptive Certificate Without Message Recovery 243
Figure F-6: Certificate Formation - Non Self Descriptive Certificate Without Message Recovery 244
Figure F-7: Certificate Formation - Self Descriptive Certificate with Message Recovery 245
Figure F-8: Certificate Formation - Non Self Descriptive Certificate with Message Recovery 246
Figure F-9: Entity Authentication Flow 247
Figure F-10: APDU C-MAC Generation 257
Figure F-11: Secure Messaging: Command message protected for confidentiality 259
Figure F-12: Secure Messaging: Command message protected for integrity and confidentiality 260
Figure F-13: Secure Messaging: Response message protected for integrity 261
Figure F-14: Secure Messaging: Response message protected for confidentiality 262
Figure F-15: Secure Messaging: Response message protected for integrity and confidentiality 264

Table 1-1: Normative References 5

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0013

Table 1-2: Terminology and Definitions 8
Table 1-3: Abbreviations and Notations 10
Table 6-1: Privileges 54
Table 6-2: Privilege Defaults 55
Table 6-3: Privilege Assignment Example Use Cases 56
Table 10-1: Current Security Level 115
Table 11-1: Authorized GlobalPlatform Commands per Card Life Cycle State 119
Table 11-2: Minimum Security Requirements for GlobalPlatform Commands 119
Table 11-3: Executable Load File Life Cycle Coding 120
Table 11-4: Application Life Cycle Coding 120
Table 11-5: Security Domain Life Cycle Coding 120
Table 11-6: Card Life Cycle Coding 120
Table 11-7: Privileges (byte 1) 121
Table 11-8: Privileges (byte 2) 121
Table 11-9: Privileges (byte 3) 121
Table 11-10: General Error Conditions 122
Table 11-11: CLA Byte Coding 122
Table 11-12: CLA Byte Coding 123
Table 11-13: Confirmation Structure 124
Table 11-14: Confirmation Data 124
Table 11-15: Implicit Selection Parameter 124
Table 11-16: Key Type Coding 125
Table 11-17: Key Usage Qualifier 126
Table 11-18: Key Access 126
Table 11-19: DELETE Command Message 128
Table 11-20: DELETE Reference Control Parameter P1 128
Table 11-21: DELETE Reference Control Parameter P2 129
Table 11-22: Delete [card content] Command Data Field 129
Table 11-23: DELETE [key] Command Data Field 129
Table 11-24: DELETE Response Data Field 130
Table 11-25: DELETE Error Conditions 130
Table 11-26: GET DATA Command Message 131

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0014

Table 11-27: Key Information Data Structure - Basic 133
Table 11-28: Key Information Data Structure - Extended 133
Table 11-29: List of On-Card Applications 133
Table 11-30: GET DATA Error Conditions 134
Table 11-31: GET STATUS Command Message 135
Table 11-32: GET STATUS Reference Control Parameter P1 135
Table 11-33: GET STATUS Reference Control Parameter P2 136
Table 11-34: GET STATUS Command Data Field 136
Table 11-35: Issuer Security Domain, Application and Executable Load File Information Data 137
Table 11-36: GlobalPlatform Registry Data (TLV) 137
Table 11-37: Executable Load File and Executable Module Information Data 138
Table 11-38: GET STATUS Warning Condition 138
Table 11-39: GET STATUS Error Conditions 139
Table 11-40: INSTALL Command Message 140
Table 11-41: INSTALL Command Reference Control Parameter P1 140
Table 11-42: INSTALL [for load] Command Data Field 142
Table 11-43: INSTALL [for install] Command Data Field 142
Table 11-44: INSTALL [for make selectable] Command Data Field 143
Table 11-45: INSTALL [for extradition] Command Data Field 144
Table 11-46: INSTALL [for registry update] Command Data Field 145
Table 11-47: INSTALL [for personalization] Command Data Field 145
Table 11-48: Load Parameter Tags 146
Table 11-49: Install Parameter Tags 147
Table 11-50: Make Selectable Parameter Tags 148
Table 11-51: Extradition Parameter Tags 148
Table 11-52: Registry Update Parameter Tags 148
Table 11-53: Values for Restrict Parameter (Tag 'D9') 149
Table 11-54: INSTALL Response Data Field 149
Table 11-55: INSTALL Error Conditions 150
Table 11-56: LOAD Command Message Structure 151
Table 11-57: LOAD Command Reference Control Parameter P1 151
Table 11-58: Load File Structure 152

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0015

Table 11-59: LOAD Response Data Field....153
Table 11-60: LOAD Error Conditions....153
Table 11-61: MANAGE CHANNEL Command Message....154
Table 11-62: MANAGE CHANNEL Warning Conditions....155
Table 11-63: MANAGE CHANNEL Error Conditions....155
Table 11-64: PUT KEY Command Message....156
Table 11-65: PUT KEY Reference Control Parameter P1....157
Table 11-66: PUT KEY Reference Control Parameter P2....157
Table 11-67: Key Version Number Diagram....157
Table 11-68: Key Data Field - Basic....158
Table 11-69: Key Data Field - Extended....159
Table 11-70: PUT KEY Error Conditions....160
Table 11-71: SELECT Command Message....161
Table 11-72: SELECT Reference Control Parameter P1....161
Table 11-73: SELECT Reference Control Parameter P2....161
Table 11-74: File Control Information....162
Table 11-75: SELECT Warning Condition....162
Table 11-76: SELECT Error Conditions....162
Table 11-77: SET STATUS Command Message....163
Table 11-78: SET STATUS – Status Type....163
Table 11-79: SET STATUS Error Conditions....164
Table 11-80: STORE DATA Command Message....166
Table 11-81: STORE DATA Reference Control Parameter P1....166
Table 11-82: STORE DATA Error Condition....168
Table C-1: Token and Receipt Keys....176
Table C-2: Additional Security Domain Key....177
Table C-3: Data Elements Included in the Load Token....179
Table C-4: Data Elements Included in the Install Token....180
Table C-5: Data Elements Included in the Make Selectable Token....181
Table C-6: Data Elements Included in the Extradition Token....182
Table C-7: Data Elements Included in the Registry Update Token....183
Table C-8: Data Elements Included in the Delete Token....184

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0016

Table C-9: Data Elements Included in the Load, Install and Make Selectable Token....186
Table C-10: Data Elements Included in the Load Receipt....187
Table C-11: Data Elements Included in the Install/Make Selectable Receipt....188
Table C-12: Data Elements Included in the Extradition Receipt....189
Table C-13: Data Elements Included in the Registry Update Receipt....190
Table C-14: Data Elements Included in the Delete Receipt....190
Table C-15: Data Elements Included in the Load, Install and Make Selectable Receipt....191
Table D-1: Security Domain Secure Channel Keys....198
Table D-2: Minimum Security Requirements for SCP01 Commands....203
Table D-3: SCP01 Command Support per Card Life Cycle State....203
Table D-4: INITIALIZE UPDATE Command Message....205
Table D-5: INITIALIZE UPDATE Response Message....206
Table D-6: INITIALIZE UPDATE Error Condition....206
Table D-7: EXTERNAL AUTHENTICATE Command Message....207
Table D-8: EXTERNAL AUTHENTICATE Reference Control Parameter P1....207
Table D-9: EXTERNAL AUTHENTICATE Error Condition....208
Table E-1: Values of Parameter "i"....209
Table E-2: SCP02 - Security Domain Secure Channel Base Key....216
Table E-3: SCP02 - Security Domain Secure Channel Keys....216
Table E-4: SCP02 Command Support....224
Table E-5: Minimum Security Requirements for SCP02 Commands....224
Table E-6: SCP02 Command Support per card Life Cycle State....224
Table E-7: INITIALIZE UPDATE Command Message....226
Table E-8: INITIALIZE UPDATE Response Message....227
Table E-9: INITIALIZE UPDATE Error Condition....227
Table E-10: EXTERNAL AUTHENTICATE Command Message....228
Table E-11: EXTERNAL AUTHENTICATE Reference Control Parameter P1....228
Table E-12: EXTERNAL AUTHENTICATE warning Code....229
Table E-13: BEGIN R-MAC SESSION Command Message....230
Table E-14: BEGIN R-MAC SESSION Reference Control Parameter P1....230
Table E-15: BEGIN R-MAC SESSION Reference Control Parameter P2....230
Table E-16: BEGIN R-MAC SESSION Command Data Field....231

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0017

Table E-17: BEGIN R-MAC SESSION Error Conditions 231
Table E-18: END R-MAC SESSION Command Message 232
Table E-19: END R-MAC SESSION Reference Control Parameter P2 232
Table E-20: END R-MAC SESSION Error Conditions 233
Table F-1: Values of Parameter "i" 235
Table F-2: Example of Data Included in Certificates 242
Table F-3: Data to Hash 248
Table F-4: Security Domain Signature Block 248
Table F-5: Data to Hash 248
Table F-6: Security Domain Signature Block 249
Table F-7: Data to Hash 249
Table F-8: Off-Card Entity Signature Block 250
Table F-9: Data to Hash 250
Table F-10: Off-Card Entity Signature Block 251
Table F-11: Single CRT 255
Table F-12: Counter Value for Session Key Calculation 256
Table F-13: SCP10 Command Support 265
Table F-14: Minimum Security Requirements for SCP10 commands 265
Table F-15: SCP10 command support per Card Life Cycle State 266
Table F-16: EXTERNAL AUTHENTICATE Command Message 267
Table F-17: Error Conditions 267
Table F-18: GET CHALLENGE Command Message 268
Table F-19: GET DATA [certificate] Command Message 269
Table F-20: GET DATA [certificate] Command Data Message 270
Table F-21: GET DATA [certificate] Response Data Field - Certificate 270
Table F-22: Error Conditions 270
Table F-23: INTERNAL AUTHENTICATE Command Message 271
Table F-24: INTERNAL AUTHENTICATE Command Data Field 271
Table F-25: Warning Conditions 272
Table F-26: Error Conditions 272
Table F-27: MANAGE SECURITY ENVIRONMENT Command Message 273
Table F-28: MANAGE SECURITY ENVIRONMENT Reference Control Parameter P1 273

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0018

Table F-29: MANAGE SECURITY ENVIRONMENT Command Data Field 274
Table F-30: Error Conditions....274
Table F-31: PERFORM SECURITY OPERATION [decipher] Command Message 275
Table F-32: Off-Card Entity Session Key Data - Clear Text before Encryption 276
Table F-33: Error Conditions....276
Table F-34: PERFORM SECURITY OPERATION [verify certificate] Command Message....277
Table F-35: PERFORM SECURITY OPERATION [verify certificate] Command Data Field....277
Table F-36: Error Conditions....278
Table H-1: Structure of Card Recognition Data 281
Table H-2: Security Domain Management Data 282

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0019

Part I
Introduction

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0021

1 Introduction

GlobalPlatform is an organization that has been established by leading companies from the payments and communications industries, the government sector and the vendor community, and is the first to promote a global infrastructure for smart card implementation across multiple industries. Its goal is to reduce barriers hindering the growth of cross-industry, multiple Application smart cards. The smart card issuers will continue to have the freedom to choose from a variety of cards, terminals and back-end systems.

For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional.

Beginning in the mid-1990s, a number of very significant breakthroughs occurred in the chip card industry with the introduction of open systems specifications for Application development. The leading technologies in this area are Java Card™ and MULTOS™. These technology specifications provide an important contribution to the solution towards the multi-Application chip card vision, such as common programming standards allowing Application portability between different card specific implementations.

Then in 2001 a PKI-based card content management framework was defined by NICSS (the Next generation IC Card System Study group) especially for the governmental sector market. The concept of NICSS is to separate the application provider from card issuer in a trusted manner whereby applications providers can 'rent' card memory space from the card issuer. This creates a new business model for each stakeholder. Additionally, in the mobile telecommunication sector ETSI have been addressing card content management 'over the air' for the secure management of the SIM and third generation UICC.

Through the Open Platform initiative, first Visa International and now GlobalPlatform have been working with the chip card industry to deliver a missing and critically important chip card standard — a hardware-neutral, vendor-neutral, Application-independent card management specification. This new specification provides a common security and card management architecture that protects the most important aspect of a chip card system investment — the infrastructure.

GlobalPlatform defines a flexible and powerful specification for Card Issuers to create single- and multi-Application chip card systems to meet the evolution of their business needs. The specification allows them to choose the card technology that is right for them today while also ensuring that they can migrate, if necessary, to a different card technology in the future without significant impact to their infrastructure.

This specification describes the GlobalPlatform Specifications that shall be implemented on GlobalPlatform smart cards.

The following meanings apply to SHALL, SHOULD, and MAY in this document:

- SHALL indicates that the statement containing the SHALL must be implemented as defined in this Specification. It does not mandate the implementation of the statement;
- SHOULD indicates a recommendation. It is strongly recommended to implement the statement as defined in this Specification;
- MAY indicates an option.

In this specification, some elements are identified as "deprecated". Such elements are no longer maintained and no evolution of these elements will be considered in the future. There is no guarantee that these elements will be present in a future release of this specification. Therefore, it is not recommended to include deprecated elements in new products or to reference them in new specification documents.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0022

1.1 Audience

This specification is intended primarily for card manufacturers and application developers developing GlobalPlatform card implementations. Although this specification defines card components, command interfaces, transaction sequences, and interfaces that can be common across many different industries, it does not detail the implementation of the lower layers security, which may vary from one industry to the other.

This specification is also intended for a more general audience as it describes the generic security concepts and the various actors involved in a multi-Application Card Management System.

1.2 IPR Disclaimer

GlobalPlatform draws attention to the fact that it is claimed that compliance with this specification may involve the use of a patent or other intellectual property right (collectively, "IPR") concerning asynchronous loading with asymmetric protocol SCP10 as described in annex F.1.1.2. GlobalPlatform takes no position concerning the evidence, validity and scope of this IPR.

Information may be obtained from:

GEMALTO
6 rue de la Verrerie
92 MeudonFrance
Phone: +33 (0) 1 55 01 50 00
Fax: +33 (0) 1 55 01 52 70
www.gemalto.com

1.3 Normative References

Standard / Specification	Description
ANSI X9.52	Triple Data Encryption Algorithm Modes of Operation, draft, 1996
CWA 14890-1	CEN Workshop Agreement - Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements, March 2004
ETSI TS 102 221 (Release 6)	Smart cards; UICC - Terminal interface; Physical and logical characteristics, European Telecommunications Standards Institute Project Smart Card Platform (EP SCP), 2004
ETSI TS 102 225 (Release 6)	Smart cards; Secured packet structure for UICC based applications, European Telecommunications Standards Institute Project Smart Card Platform (EP SCP), 2004
ETSI TS 102 226 (Release 6)	Smart cards; Remote APDU structure for UICC based applications, European Telecommunications Standards Institute Project Smart Card Platform (EP SCP), 2004
ETSI TS 102 241 (Release 6)	Smart cards; UICC Application Programming Interface (UICC API) for Java Card™, European Telecommunications Standards Institute Project Smart Card Platform (EP SCP), 2004

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0023

Standard / Specification	Description
FIPS PUB 180-2	Federal Information Processing Standards Publication 180-2, 2002: Specifications for the Secure Hash Standard: U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology
FIPS PUB 197	Federal Information Processing Standards Publication 197, 2001: Specification for the Advanced Encryption Standard (AES): U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology
FIPS PUB 198	Federal Information Processing Standards Publication 198, 2002: Standard for the Keyed-Hash Message Authentication Code (HMAC): U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology
GlobalPlatform KMS	GlobalPlatform Key Management System Functional Requirements, version 1.0
GlobalPlatform MS	GlobalPlatform Messaging Specification, version 1.0
GlobalPlatform SCMS	GlobalPlatform Smart Card Management System Functional Requirements, version 4.0
GlobalPlatform Systems Scripting Language Specification	GlobalPlatform Systems Scripting Language Specification, version 1.1.0
ISO/IEC 7816-3:1997	Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols
ISO/IEC 7816-4:2005	Identification cards – Integrated circuit cards - Part 4: Organization, security and commands for interchange
ISO/IEC 7816-6:2004	Identification cards - Integrated circuit(s) cards with contacts- Part 6: Interindustry data elements
ISO/IEC 7816-15:2004	Identification cards - Integrated circuit cards with contacts - Part 15: Cryptographic information application
ISO 8731-1:1987	[IS8731-1] Banking - Approved algorithms for message authentication – Part 1: DEA
ISO/IEC 8825-1:2002 | ITU-T Recommendation X.690 (2002)	Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
ISO/IEC 9594-8 | ITU-T Recommendation X.509 (2000)	Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks
ISO/IEC 9796-2:2002	Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms
ISO/IEC 9797:1994	[IS9797] Information technology – Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
ISO/IEC 9899:1999	Programming languages - C
ISO/IEC 10116: 1997	[IS10116] Information technology - Modes of operation of an n-bit block cipher algorithm

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0024

Standard / Specification	Description
ISO/IEC 10118-3: 1998	[IS10118-3] Information technology – Security techniques - Hash functions –Part 3: Dedicated hash functions
ISO/IEC 14443-3:2001	Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision
ISO/IEC 14443-4:2001	Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol
ISO/IEC 18033-3:2005	Information Technology - Security techniques - Encryption algorithms - Part 3: Block ciphers
Java Card™	Go to the following website for Java Card™ documentation: http://java.sun.com/products/javacard
MAO-DOC-REF-009	MULTOS Guide to Generating Application Load Units, version 2.51
MULTOS™	Go to the following website for MULTOS™ documentation: http://www.multos.com
NICSS Framework (NICSS-F)	NICSS Prerequisites, First Edition, version 1.20, April 24, 2001, The Next generation IC Card System Study group
PKCS#1	PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002.
GlobalPlatform Card Specification v2.2 Amendment C	GlobalPlatform Card Specification v2.2 Amendment C v1.0 – Contactless Services

Table 1-1: Normative References

1.4 Terminology and Definitions

Table 1-2 defines the expressions used within this Specification that use an upper case first letter in each word of the expression. Expressions within this document that use a lower case first letter in each word take the common sense meaning. (Tagged data elements are also given an upper case first letter in each word of their names.)

Term	Definition
Application	Instance of an Executable Module after it has been installed and made selectable
Application Management System	An off-card application-specific system required to successfully implement an Application Provider's service to a cardholder
Application Protocol Data Unit (APDU)	Standard communication messaging protocol between a card accepting device and a smart card
Application Provider	Entity that owns an application and is responsible for the application's behavior
Application Session	The link between the Application and the external world on a logical channel starting with the selection of the Application and ending when the same or another Application is selected on the logical channel, the logical channel is closed or the Card Session terminates

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0025

Term	Definition
Asymmetric Cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the Public Key component) and a private transformation (defined by the Private Key component); these two key components have a property so that it is computationally infeasible to discover the Private Key, even if given the Public Key
Basic Logical Channel	The permanently available interface between the card and an external entity. The Basic Logical Channel is numbered zero
Card Content	Code and Application information (but not Application data) contained in the card that is under the responsibility of the OPEN e.g. Executable Load Files, Application instances, etc.
Card Image Number (CIN)	An identifier for a specific GlobalPlatform card
Card Issuer	Entity that owns the card and is ultimately responsible for the behavior of the card
Card Management System	An off-card system providing functions to manage various card types and their associated application(s)and specific configurations for cardholders
Card Manager	Generic term for the card management entities of a GlobalPlatform card i.e. the OPEN, Issuer Security Domain and a Cardholder Verification Method services provider
Card Recognition Data	Information that tells an external system, in particular a Smart Card Management System (SCMS), how to work with the card (including indicating that this is a GlobalPlatform card)
Card Session	The link between the card and the external world starting at card reset (contact cards), activation (contactless cards) or power on of the card and ending with a subsequent reset (contact cards), deactivation (contactless cards) or power off of the card
Card Unique Data	Data that uniquely identifies a card being the concatenation of the Issuer Identification Number and Card Image Number
Cardholder	The end user of a card
Cardholder Verification Method (CVM)	A method to ensure that the person presenting the card is the person to whom the card was issued
Certificate	In this Specification, a Certificate refers to a key certificate: the public key and identity of an entity together with some other information, rendered unforgeable by signing with the private key of the certification authority which issued that Certificate.
Controlling Authority	A Controlling Authority has the privilege to keep the control over the Card Content through the mandating of DAP Verification
Current Security Level	A level of security that is to be applied to the current command-response pair in a Secure Channel Protocol using secure messaging. It is set for an individual command (APDU pair): the current incoming command APDU and the next response.
DAP Block	Part of the Load File used for ensuring Load File Data Block verification
DAP Verification	A mechanism used by a Security Domain to verify that a Load File Data Block is authentic
Delegated Management	Pre-authorized Card Content changes performed by an approved Application Provider

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0026

Term	Definition
Digital Signature	A cryptographic transformation of data that allows the recipient of the data to prove the origin and integrity of the data; it protects the sender and the recipient of the data against forgery by third parties; it also protects the sender against forgery by the recipient
Executable Load File	Actual on-card container of one or more application's executable code (Executable Modules). It may reside in Immutable Persistent Memory or may be created in Mutable Persistent Memory as the resulting image of a Load File Data Block
Executable Module	Contains the on-card executable code of a single application present within an Executable Load File
GlobalPlatform Registry	A container of information related to Card Content management
Host	A logical term used to represent the back end systems that support the GlobalPlatform system; hosts perform functions such as authorization and authentication, administration, Post-Issuance application code and data downloading, and transactional processing
Immutable Persistent Memory	Memory that can only be read
Issuer Security Domain	The primary on-card entity providing support for the control, security, and communication requirements of the card administrator (typically the Card Issuer)
Life Cycle	The existence of Card Content on a GlobalPlatform card and the various stages of this existence where applicable; or the stages in the life of the card itself
Life Cycle State	A specific state within the Life Cycle of the card or of Card Content
Load File	A file transferred to a GlobalPlatform card that contains a Load File Data Block and possibly one or more DAP Blocks
Load File Data Block	Part of the Load File that contains one or more application(s) or libraries and support information for the application(s) as required by the specific platform
Load File Data Block Hash	A value providing integrity for the Load File Data Block
Load File Data Block Signature	A value encompassing the Load File Data Block Hash and providing both integrity and authenticity of the Load File Data Block
Message Authentication Code (MAC)	A symmetric cryptographic transformation of data that provides data origin authentication and data integrity
Mutable Persistent Memory	Memory that can be modified
OPEN	The central on-card administrator that owns the GlobalPlatform Registry
Post-Issuance	Phase following the card being issued to the Cardholder
Pre-Issuance	Phase prior to the card being issued to the Cardholder
Private Key	The private component of the asymmetric key pair
Public Key	The public component of the asymmetric key pair
Receipt	An cryptographic value provided by the card (if so required by the Card Issuer) as proof that a Delegated Management operation has occurred
Retry Counter	A counter, used in conjunction with the Retry Limit, to determine when attempts to present a CVM value shall be prohibited
Retry Limit	The maximum number of times an invalid CVM value can be presented prior to the CVM prohibiting further attempts to present a CVM value

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0027

Term	Definition
Runtime Environment	Functionality on a card which provides a secure environment for multiple applications to operate. Its role is complementary to that of the GlobalPlatform Card Manager
Secure Channel	A communication mechanism between an off-card entity and a card that provides a level of assurance, to one or both entities
Secure Channel Protocol	A secure communication protocol and set of security services
Secure Channel Session	A session, during an Application Session, starting with the Secure Channel initiation and ending with a Secure Channel termination or termination of either the Application Session or Card Session
Security Domain	On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the Card Issuer, an Application Provider or a Controlling Authority)
Session Security Level	A mandatory minimum level of security to be applied to protected commands in a Secure Channel Protocol using secure messaging. It is established during the initialization of the Secure Channel Session, either explicitly or implicitly.
Supplementary Logical Channel	Up to 19 additional interfaces (other than the permanently available Basic Logical Channel) between the card and an external entity. Each Supplementary Logical Channel is numbered from 1 up to 19
Supplementary Security Domain	A Security Domain other than the Issuer Security Domain
Symmetric Cryptography	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation
Token	A cryptographic value provided by a Card Issuer as proof that a Delegated Management operation has been authorized
Trust Point	An authority whose public key is trusted by a Security Domain or Off-Card Entity through some undefined mechanism such as a secure process that delivers the public key in a self-signed certificate. A Trust Point's public key is typically the 'highest' public key known to the entity.
UICC	The ICC as defined by ETSI Project Smart Card Platform (EP SCP)

Table 1-2: Terminology and Definitions

1.5 Abbreviations and Notations

Abbreviation	Meaning
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ATR	Answer-to-Reset
ATQ	Answer-to-Request (for contactless cards)
BCD	Binary Coded Decimal
BER	Basic Encoding Rules

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0028

Abbreviation	Meaning
CAT	Card Application Toolkit; or Cryptographic Authorization Template
CBC	Cipher Block Chaining
CCT	Control Reference Template for Cryptographic Checksum
CIN	Card Image Number / Card Identification Number
CLA	Class byte of the command message
CRT	Control Reference Template
CT	Control Reference Template for Confidentiality
CVM	Cardholder Verification Method
DAP	Data Authentication Pattern
DEK	Data Encryption Key
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DST	Control Reference Template for Digital Signature
ECB	Electronic Code Book
EMV	Europay, MasterCard, and Visa; used to refer to the ICC Specifications for Payment Systems
ENC	Encryption
FCI	File Control Information
HEX	Hexadecimal
HMAC	Keyed-Hash Message Authentication Code
ICC	Integrated Circuit Card
ICV	Initial Chaining Vector
IIN	Issuer Identification Number
INS	Instruction byte of the command message
ISO	International Organization for Standardization
Lc	Exact length of data in a case 3 or case 4 command
Le	Maximum length of data expected in response to a case 2 or case 4 command
LV	Length Value
MAC	Message Authentication Code
MEL	MULTOS Executable Language. The instruction set of the MULTOS™ runtime environment
OID	Object Identifier
P1	Reference control parameter 1
P2	Reference control parameter 2
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RAM	Random Access Memory
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
ROM	Read-only Memory
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SCP	Secure Channel Protocol; or (ETSI) Smart Card Platform
SW	Status Word
SW1	Status Word One
SW2	Status Word Two

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0029

Abbreviation	Meaning
TLV	Tag Length Value
TP	Trust Point
'xx'	Hexadecimal values are expressed as hexadecimal digits between single quotation marks
'X'	A value in a cell of a table whose purpose is described in the 'meaning' column of the table
'-'	A value (0 or 1) in a cell of a table that does not affect the 'meaning' given for that row of the table

Table 1-3: Abbreviations and Notations

1.6 Revisions History

1.6.1 Open Platform Card Specification v2.0 to Open Platform Card Specification v2.0.1

This section provides a brief summary of the revisions made to the Open Platform Card Specification 2.0 Card Specification in the Open Platform Card Specification 2.0.1'.

Wording and formatting of the specification had been improved.

Anything relating to a specific implementation of Open Platform had been removed from the main body of the specification and was detailed in the appendices.

Anything specific relating to the personalization of Open Platform or Applications had been removed.

The changes relating specifically to the Java Card™ implementation of Open Platform were listed in the beginning of appendix A - *GlobalPlatform API*.

All the issues identified in the FAQ document dated April-June 1999 and the FAQ documents dated October-November 1999 and relating strictly to Open Platform, had been included in this version. The one caveat to this was the point 3.1.20 of the FAQ document dated October-November 1999 i.e. it is now required that the Security Domain associated with an Application be the same Security Domain used to perform Delegated Management functions for this Application.

The inclusion of Part V described a specific use of security and key management that was not present in Open Platform 2.0.

1.6.2 Major Adjustments in GlobalPlatform Card Specification v2.1

The following major adjustments are the modifications decided by GlobalPlatform Members. All of these modifications are intended to make the GlobalPlatform more usable for a wider number of entities while maintaining backwards compatibility. The minor editing changes and rewording for readability are not listed.

1.6.2.1 Enhancement to DAP Verification Scheme

In the process of implementing GlobalPlatform cards that supported Delegated Management and DAP Verification, it was determined that the method defined in the previous version of Open Platform necessitated the verification of multiple signatures on large blocks of data (Load File and Load File Data Block) that differed only slightly. When multiple DAP Verifications and possibly Delegated Management was being performed simultaneously, multiple hash generations were required to run concurrently. This negatively impacted the performance of the load process.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0030

A new method has been defined in which instead of signing large blocks of data, a hash of the critical large block of data (Load File Data Block) may be generated and this hash signed. In this new method signatures are required on very much smaller blocks of information. Only one hash generation and check is required on the Load File Data Block.

1.6.2.2 Application Reception of Data from Security Domains

The Secure Channel mechanism previously provided by Open Platform only allowed an Application to request services from its associated Security Domain.

A new service is now provided that may be initiated by a Security Domain. It allows data to be passed by the Security Domain associated with an Application to the Application for further processing. The main purpose of this service is to facilitate the personalization of Applications through the Applications' associated Security Domain. A new INSTALL command has been defined to identify the Application to be personalized.

1.6.2.3 Security Domain Association and Extradition

In the previous Open Platform Card Specification an Executable Load File was associated with a Security Domain and all Applications instantiated from an Executable Load file, when installed, were also associated with the same Security Domain. This method was restrictive.

The new scheme provides Application Extradition. Application Extradition allows an Application that is already associated with a Security Domain to be extradited and associated with another Security Domain.

Another benefit provided by this enhancement is that in addition to Executable Load Files and Applications, now applications within Executable Load Files become visible in the GlobalPlatform Registry at the time that the Executable Load File is registered.

In order to avoid confusion between selectable Applications and the applications within an Executable Load File a new term has been introduced i.e. Executable Module. The term Executable Module is intended to identify the one or more applications present within an Executable Load File.

1.6.2.4 Executable Modules

In the previous Open Platform Card Specification, an off-card entity could only retrieve information relating to the Executable Load Files and selectable Applications present on the card. In order to enhance the information returned by the GET STATUS command, an additional set of information will be stored in the GlobalPlatform Registry and returned in the response to the GET STATUS command. This information relates to the Executable Module and it is now possible to also retrieve information relating to application code within an Executable Load File that is available for installation.

1.6.2.5 Card Recognition Data

A concerted effort was made to ensure that there would be a uniform method to determine basic information about a card. The Card Recognition Data and the method for retrieving this data have been included in this version of the GlobalPlatform Card Specification. Information such as: this is a GlobalPlatform card, implemented in a particular way, and with a particular version number is now available.

1.6.2.6 Support of New Secure Channel Protocols

In order to be more accommodating, the method for including additional Secure Channel Protocols has been formalized. While this was allowed in previous versions of the Open Platform Card Specification, only one Secure Channel Protocol was defined. As part of the efforts of GlobalPlatform a formal process

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0031

for including Secure Channel Protocols is defined. This version of the specification details two Secure Channel Protocols and their selection process. To provide clarity a slight re-organization of the GlobalPlatform Card specification has been done. Part V of the Open Platform 2.0.1' specification has been removed. Part of its content is incorporated into Part III and the rest is moved into the appendices.

1.6.2.7 Cardholder Verification Method Services

Additional services and features regarding the optional CVM have been included. In the previous versions of the Open Platform Card Specification, the CVM provided the possibility for a single PIN to be common across multiple Applications. When the PIN was changed by one Application it became visible to all Applications. However an Application could not check whether the PIN had previously been correctly presented to another Application during the same Card Session. The new Card Verification Method (CVM) services provide the ability to do this check.

1.6.2.8 Card Manager Separation

Historically the Card Manager has been viewed and defined as the major on-card component with no distinction or separation between the various responsibilities encompassed within as well as not clearly defining where the runtime environment ends and the Card Manager begins. A decision has been made to separate the Card Manager into 3 distinct entities and clearly identifying what runtime environment functionality must be within each. While the term Card Manager is still present, it now encompasses the OPEN, the Issuer Security Domain and the Cardholder Verification Method Services provider. This new structure clarifies the responsibilities of the Card Manager and takes into account both Java Card and Windows Powered Smart Card.

1.6.2.9 Windows Powered Smart Card API

The GlobalPlatform API for Windows Powered Smart Card is now included.

1.6.2.10 Java Card API

Taking into account the various new features of the GlobalPlatform a new API providing support for these new, and all relevant existing, features has been specified for Java Card. The previous Open Platform API for Java Card defined in version 2.0.1' is deprecated and remains in this version for backward compatibility.

1.6.2.11 Appendices

The body of the GlobalPlatform Card Specification only contains generic GlobalPlatform descriptions. All information specific to a particular implementation has been positioned in a set of appendices.

1.6.3 Revisions in GlobalPlatform Card Specification v2.1.1

The following modifications correct issues in the previous version and synchronize with recent evolutions of the underlying runtime environment specifications while maintaining full backwards compatibility. The minor editing changes and rewording for readability are not listed.

1.6.3.1 Errata

All intermediate published errata have been incorporated into this version. There is also a small set of errata and precisions that would have been published at around the same time this version is released, and these have also been incorporated directly into this version.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0032

1.6.3.2 Content Removal

A new optional Card Content removal feature has been added that allows an Executable Load File and all its related Applications to be deleted in the same operation.

1.6.3.3 Logical Channels

To meet the emerging needs of some industries and recent evolutions of the underlying runtime environment specifications, logical channel functionality is added to this version of the specification as an optional feature.

1.6.3.4 Additional Secure Channel Protocol Implementation Options

An enhanced mechanism of generating a C-MAC has been added to both Secure Channel Protocol '01' and Secure Channel Protocol '02'. One new implementation option has been added for Secure Channel Protocol '01' and four new implementation options have been added for Secure Channel Protocol '02'. It is recommended that these new implementation options be used.

1.6.4 Major Adjustments in GlobalPlatform Card Specification v2.2

The following major adjustments are modifications decided by GlobalPlatform Members. All of these modifications are intended to make the GlobalPlatform more usable for a wider number of entities while maintaining full backward compatibility with previous versions.

The body of the document has been reorganized to reflect these changes, to arrange it by functions and components as well as to remove excessive duplication.

1.6.4.1 PKI functionality and Card Content Management

Card Content Management may now be performed by relying exclusively on asymmetric cryptography and a Public Key Infrastructure. This has resulted in the need to formalize the process of authentication and establishing ownership, so that the card can apply the relevant security and authorization rules for different off-card entities.

A delete token is added as an option, so that the Card Issuer may have a PK based policy to authorize card content removal.

1.6.4.2 Over-The Air Functionality and Inter-Application Communication

A mechanism for inter-application communication is formalized in terms of a general framework: Trusted Framework, which encompasses both the GlobalPlatform mechanism whereby an Application could receive its personalization data from its Security Domain as well as the SIM Toolkit and CAT frameworks defined for UICC cards by ETSI Project Smart Card Platform specifications. A new privilege - Trusted Path - between an on-card Receiving Entity and an on-card target Application is introduced.

1.6.4.3 Contactless Cards, Implicit Selection and Logical Channels

Support for contactless cards and dual interface cards (contact and contactless) is made more explicit in this version.

With the introduction of a new installation parameter, different Applications can now be implicitly selected on different card I/O interfaces: contact or contactless (and potentially others), and different logical channels.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0033

The Default Selected privilege is redefined as the Card Reset privilege to modify the historical bytes. An Application is able to refuse explicit selection, e.g. because it does not support the current card I/O interface, and allow the (partial) selection process by OPEN to continue. To provide backward compatibility, the privilege confers implicit selectability if it has not been awarded to another Application.

As a further option, support of logical channels is expanded up to 19 supplementary logical channels as defined by the latest version of ISO/IEC 7816-4.

1.6.4.4 Secure Channel Protocols

A new Secure Channel Protocol based on asymmetric cryptography and a Public Key Infrastructure is introduced as Secure Channel Protocol '10'. Secure Channel Protocol '10' is compatible with CEN Workshop Agreement specification CWA 14890-1. It also fulfills the requirements of NICSS Framework Scheme defined by the Next Generation IC Card System Study Group (NICSS).

This version references the Secure Channel Protocol defined by ETSI Project Smart Card Platform TS 102 225 specification as GlobalPlatform Secure Channel Protocol '80'.

The number of recommended options for Secure Channel Protocol '02' is reduced to the most commonly used ones. The option indicator for Secure Channel Protocol '02' is defined as a bit-map and allows the support of any other option that was described in version 2.1.1 or Amendment A.

Secure Channel Protocol '01' is now deprecated.

The use of Security Levels associated with a secure channel session and an individual command-response pair have been made more explicit in this version. This version provides improved API support for Secure Channel Protocols. For example, an Application has the ability to increase the security level required for a (sequence of) individual command-response pair(s) using the GlobalPlatform API.

1.6.4.5 Global Services and CVMs

A general framework for dynamic management of card-wide services is introduced whereby one or more Global Services Applications may be present on a card to provide services to other Applications. The Global Services Applications are distinguished by having the Global Service privilege. A new installation parameter allows the on-card registration of service parameters. Service parameters are standardized by GlobalPlatform and can be registered as unique on the card by Global Services Applications using the GlobalPlatform API. GlobalPlatform API extensions allow Applications to request and, if authorized, use the services offered by Global Services Applications.

CVM functions are devolved from the OPEN to separate CVM Applications as Global Services Applications. Each CVM Application can handle one or multiple CVMs. GlobalPlatform API extensions allow CVM Applications to establish whether Applications have the authority to use and/or modify CVMs. Backward compatibility of the GlobalPlatform API is ensured for existing Applications using CVM services.

1.6.4.6 Security Domains, Privileges and Hierarchies

The privileges associated with Security Domains, in particular the Issuer Security Domain, are formalized so that access rights to Card Content Management functionality are more explicit. The Issuer Security Domain now has an explicit set of privileges, including new privileges such as Authorized Management or Token Verification. Other new privileges are introduced to formalize the access rights awarded to Security Domains and Applications such as Global Registry Access, Global Lock and Global Delete.

Security Domain and Application privileges can now be modified dynamically on the card during their lifetime. CVM identifiers are standardized by GlobalPlatform.

Security Domains and OPEN itself can now have their Card Content Management functionality restricted dynamically during their Life Cycle through the use of a new INSTALL command.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0034

Security Domains can now be associated with other Security Domains and so create a hierarchy of Security Domains. Association with Security Domains is made more systematic, so that a hierarchy of control can be established through association and extradition. Multiple hierarchies of Security Domains can be established, including by extraditing a Security Domain to itself and so making it the root of a new hierarchy. Access rights of Security Domains to Card Content Management functionality are expressed in regard to their association and hierarchy.

Card Content Management functionality has been extended to include explicit extradition of Executable Load Files.

The Token Verification privilege and the Receipt Generation privilege have been added.

1.6.4.7 On-Card APIs for Applications

A GlobalPlatform API expressed in the 'C' programming language for MULTOS™ cards is now included.

The GlobalPlatform API has been expanded and enhanced in order to support the new functionality introduced in this version.

References to Windows Powered Smart Card, and its specific API, have been deleted from this version.

The deprecated Open Platform Java Card API has also been removed from this version.

1.6.4.8 Key Management

New optional attributes for cryptographic keys are added to allow for more control, and for the partitioning of keys with different purposes. The new attributes are key usage and key access condition.

New key types are also added to support new cryptographic algorithms.

1.6.4.9 Amendment A

Amendment A to version 2.1.1 has been incorporated into this version. It comprises a set of optional extensions in support of GlobalPlatform Scripting Specification, EMV Card Personalization Specification and ETSI Project Smart Card Platform TS 102.225 and TS 102 226 specifications.

1.6.4.10 Errata and Precisions

All errata and precisions published since the release of version 2.1.1 and Amendment A have been incorporated into this version.

1.6.4.11 Other Major Changes

New installation parameters are added to further card memory management and allow memory reservation.

The Get Data command can now be used to retrieve a list of Applications present on the card.

It is now possible to lock, and subsequently unlock, a Security Domain and all its associated Applications in a single command.

It is now possible to load, install and make selectable an Application in a single combined process.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0035

1.6.5 Minor Adjustments in GlobalPlatform Card Specification v2.2.1

1.6.5.1 Errata and Precisions

All errata and precisions published since the release of version 2.2 have been incorporated into this version. Additionally, relevant errata and precisions recorded during the development of the GlobalPlatform Card UICC Configuration v1.0 and v1.0.1 have been incorporated into this version and the corresponding API.

The GlobalPlatform API specifications (Java Card™ and MULTOS™) have been removed from this document and are now published separately on the GlobalPlatform website.

1.6.5.2 Amendment A, Confidential Card Content Management v1.0 and its Errata and Precision v1.0

Items from GlobalPlatform Card Specification v2.2 Amendment A Confidential Card Content Management v1.0, sections 4.8 and 4.9 are applied to this revision.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0036

Part II
Architecture

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0037

2 System Architecture

Deploying a large number of chip cards based on dynamic, multi-application technology is not unlike deploying a very large number of workstations in a vast, semi-connected network. These card-based workstations support several different applications at any one time as well as allow for the possibility of updating or deleting those applications and installing new applications at any point in time.

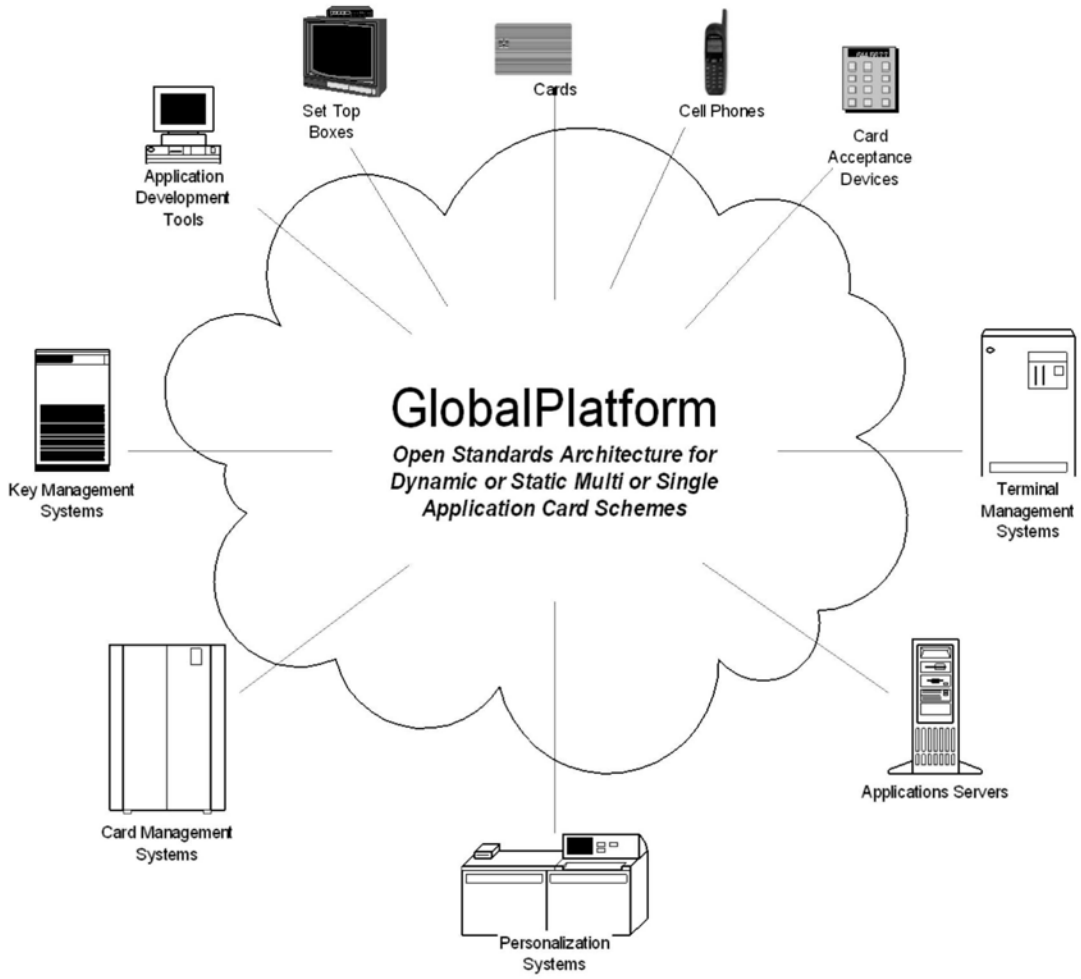


Figure 2-1: GlobalPlatform Architecture

The GlobalPlatform architecture is designed to provide Card Issuers with the system management architecture for managing these smart cards. Although GlobalPlatform is based on the paradigm that there is one single Card Issuer for a card, it offers to the Card Issuer the flexibility for managing an ever-changing array of business partners who may want to run applications on the Card Issuer's cards.

GlobalPlatform gives Card Issuers the power to manage their cards with the ultimate flexibility by enabling them to share control over part of their card with business partners. The ultimate control always rests with the Card Issuer, but through GlobalPlatform, the business partners of a Card Issuer can be allowed to manage their own Applications on the Card Issuer's cards as appropriate.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0038

3 Card Architecture

The GlobalPlatform card architecture is comprised of a number of components that ensure hardware and vendor-neutral interfaces to Applications and off-card management systems. The following figure shows the components in a sample card configuration which includes one or more applications from the Card Issuer; one or more applications from one of the business partners of the Card Issuer, referred to as Application Providers; and one or more applications providing global services (e.g. CVM services) to other applications.

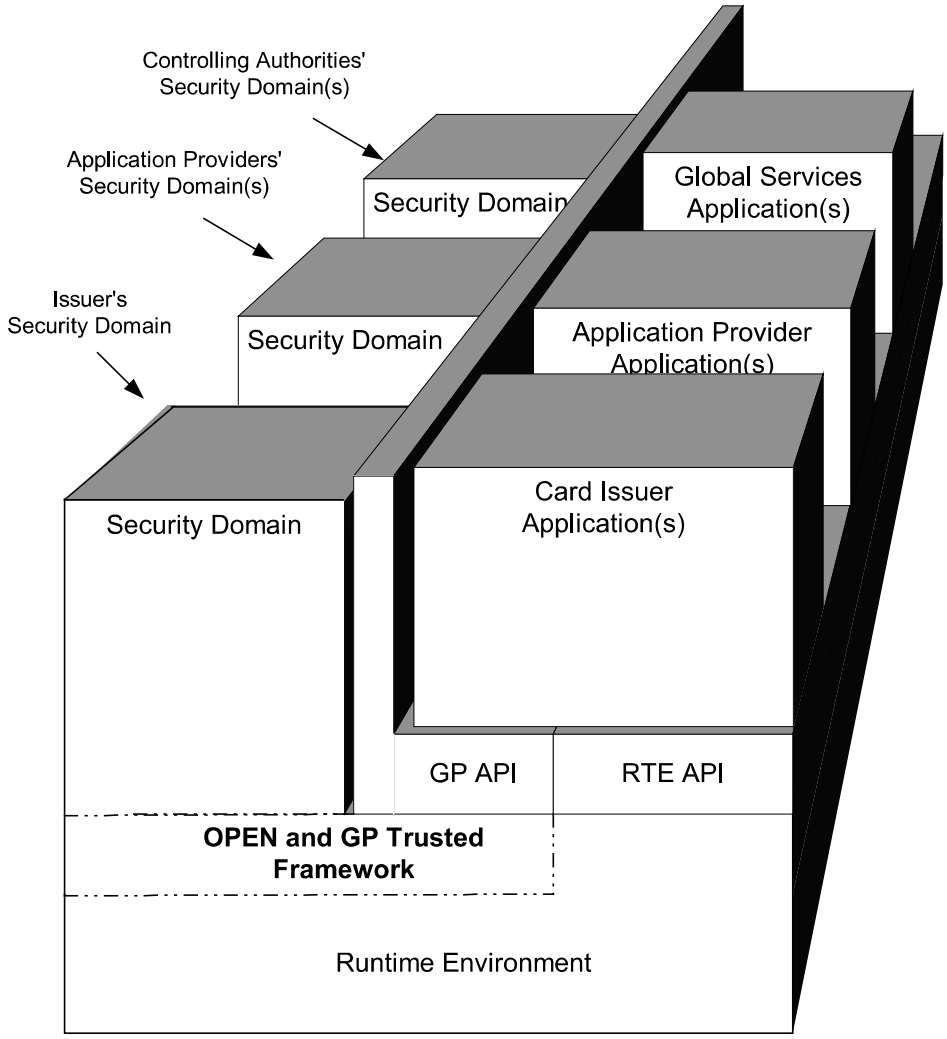


Figure 3-1: GlobalPlatform Card Architecture

All applications shall be implemented in a secure runtime environment that includes a hardware-neutral Application Programming Interface (API) to support application portability. GlobalPlatform does not mandate a specific runtime environment technology. The Card Manager is the primary GlobalPlatform card component that acts as the central administrator for a GlobalPlatform card. Special key and security

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0039

management applications called Security Domains are created to ensure complete separation of keys between the Card Issuer and multiple other Security Domain providers.

3.1 Security Domains

Security Domains act as the on-card representatives of off-card authorities. There are three main types of Security Domain, reflecting the three types of off-card authority recognized by a card:

- The Issuer Security Domain is the primary, mandatory on-card representative of the Card Administrator, typically the Card Issuer;
- Supplementary Security Domains are additional, optional on-card representatives of Application Providers or the Card Issuer; or their agents (e.g. service bureaus);
- Controlling Authority Security Domains are a special type of Supplementary Security Domain. A Controlling Authority may exist whose role is to enforce the security policy on all application code loaded to the card. If so, the Controlling Authority also uses this type of Security Domain as its on-card representative. There may be more than one such Security Domain.

In the main, all three types are referred to simply as Security Domains in this Specification;

Security Domains support security services such as key handling, encryption, decryption, digital signature generation and verification for their providers' (Card Issuer, Application Provider or Controlling Authority) applications.

Each Security Domain is established on behalf of a Card Issuer, an Application Provider or a Controlling Authority when these off-card entities require the use of keys that are completely isolated from each other.

3.2 Global Services Applications

One or more Global Services Applications may be present on the card to provide services to other Applications on the card. Examples of such services are Cardholder Verification Method services.

3.3 Runtime Environment

The GlobalPlatform is intended to run on top of any secure, multi-application card runtime environment. This runtime environment is responsible for providing a hardware-neutral API for applications as well as a secure storage and execution space for applications to ensure that each application's code and data can remain separate and secure from other applications on the card. The card's runtime environment is also responsible for providing communication services between the card and off-card entities.

Cards should comply with appropriate standards: ISO/IEC 7816-3, ISO/IEC 7816-4, ISO/IEC 14443-3 and ISO/IEC 14443-4 in terms of announcing options supported in the ATR/ATQ such as the communications protocol, logical channels and command chaining.

3.4 Trusted Framework

GlobalPlatform cards may contain one or more Trusted Frameworks, which provide inter-application communication services between Applications. Trusted Frameworks are not Applications or Security Domains, but have a special status in that they are part of or extensions of the card's run-time environment. They should be assessed for security similarly to the runtime environment's security assessment. See appendix G - *Trusted Framework Inter-Application Communication* for further details.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0040

3.5 GlobalPlatform Environment (OPEN)

The main responsibilities of the GlobalPlatform Environment (OPEN) are to provide an API to applications, command dispatch, Application selection, (optional) logical channel management, and Card Content management. These functions shall be implemented by the OPEN if the runtime environment does not provide them, or if they are provided by the runtime environment in a way that is not compliant with this Specification.

The OPEN performs the application code loading and related Card Content management and memory management.

The OPEN also manages the installation of applications loaded to the card. The OPEN is responsible for enforcing security principles defined for Card Content management.

Another important function provided by the OPEN is APDU command dispatching and Application selection. When a SELECT command is successfully processed, the OPEN sets the Application referenced in the SELECT command to be the selected Application and subsequent Application commands shall be dispatched to the selected Application.

The availability of logical channels introduces an additional dimension to the card's architecture as multiple Applications may be selected concurrently. The OPEN shall rely on the runtime environment to control whether and when an individual Application can be selected concurrently with itself or another Application. When supporting logical channels, the OPEN shall allow for Applications that have no notion of logical channels as well as those that are multi-selectable. Support of logical channels is optional. Cards may support one or more (up to 19 according to ISO/IEC 7816-4) Supplementary Logical Channels.

The OPEN owns and uses an internal GlobalPlatform Registry as an information resource for Card Content management. The GlobalPlatform Registry contains information for managing the card, Executable Load Files, Applications, Security Domain associations, and privileges.

3.6 GlobalPlatform API

The GlobalPlatform API provides services to Applications (e.g. Cardholder verification, personalization, or security services). It also provides Card Content management services (e.g. card locking or Application Life Cycle State update) to Applications.

For the specification of the Application Programming Interface (API) on a Java Card™, see appendix A.1.

For the specification of the Application Programming Interface (API) on a MULTOS™ card, see appendix A.2.

3.7 Card Content

All Card Content, as defined in this specification, is first available on the card in the form of an Executable Load File. An Executable Load File can either exist in:

- Immutable Persistent Memory in which case it is loaded during the manufacturing stage and cannot be altered (except being disabled); or
- Mutable Persistent Memory in which case it can be loaded, or removed during Pre-Issuance or Post-Issuance.

Each Executable Load File may contain one or multiple Executable Modules, being application code. The installation of an Application creates an instance from an Executable Module plus possibly Application data within Mutable Persistent Memory. Any Application instance and its related data can be removed. A GlobalPlatform card is intended to support multiple Executable Load Files and multiple Executable

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0041

Modules and as such multiple Applications may co-exist on a GlobalPlatform card. Note that the foregoing description assumes that Executable Modules will be present in the Executable Load File: however, their presence is optional and depends on the requirements of the Runtime Environment.

Figure 3-2 represents the relationship between an Executable Load File, an Executable Module (in the case where Executable Modules are present) and an Application.

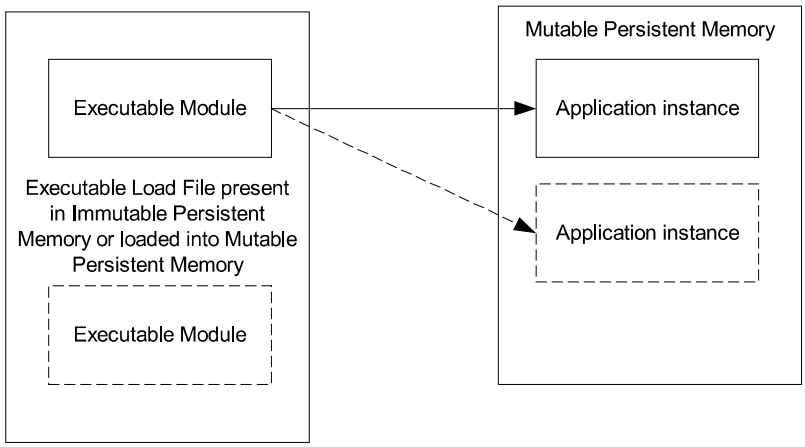


Figure 3-2 Card Content Relationships

3.8 Card Manager

The Card Manager, as the central administrator of the card, assumes multiple responsibilities.

The Card Manager can be viewed as three entities:

- The GlobalPlatform Environment (OPEN);
- The Issuer Security Domain; and
- Cardholder Verification Method Services.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0042

4 Security Architecture

Well-designed security architectures are crucial to protecting the structure and function of cards within the GlobalPlatform system.

This chapter outlines:

- The security goals behind the architecture;
- The specific responsibilities of the Card Issuer as the owner of the card;
- The Application Providers as the owners of the Applications;
- The Controlling Authority;
- The security requirements for the on-card components;
- The cryptographic support provided by GlobalPlatform

4.1 Goals

The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card. These components are

- The runtime environment;
- The OPEN;
- The Issuer Security Domain;
- Supplementary Security Domains;
- The Applications.

To ensure card security and integrity, the GlobalPlatform is designed to support a range of secure mechanisms for:

- Data integrity;
- Resource availability;
- Confidentiality;
- Authentication.

The choice of security policy and cryptography is assumed to be industry and product specific.

Because the cards are only part of a larger card system involving multiple parties and off-card components, the GlobalPlatform also relies upon non-cryptographic, procedural means of protection, such as code testing and verification, physical security, and secure key handling. However, these aspects are out of scope for this card specification.

4.2 Security Responsibilities and Requirements

4.2.1 Card Issuer's Security Responsibilities

The Card Issuer is responsible for:

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0043

- Generating and loading the Issuer Security Domain keys;
- Enforcing standards and policies for Application Providers governing all aspects of Applications to be provided to the Card Issuer or operated on the Card Issuer's cards;
- Working with Application Providers to create and initialize Security Domains other than the Issuer Security Domain;
- Determining policy with regards to card and Application Life Cycle management, velocity checking levels, privileges, and other security parameters;
- Managing the application code loading and installing both on a Pre-Issuance and Post-Issuance basis, and
- Cryptographically authorizing load, install, and extradition to be performed by Application Providers.

4.2.2 Application Provider's Security Responsibilities

The Application Provider is responsible for:

- Generating the keys for its own Security Domains or obtaining Security Domain keys from a trusted third party;
- Working with the Card Issuer to load generated keys into the Application Provider's Security Domain;
- Providing applications that meet the Card Issuer's security standards and policies;
- Providing load file data block signatures according to its own security policy for integrity and source authenticity;
- Obtaining pre-authorization for load, install, and extradition from the Card Issuer;
- Returning receipts for load, install, delete, and extradition, according to the Card Issuer's policy.

4.2.3 Controlling Authority's Security Responsibilities

A Controlling Authority is responsible for:

- Generating the keys for its own Security Domain or obtaining Security Domain keys from a trusted third party;
- Working with the Card Issuer to load generated keys into the Controlling Authority's Security Domain;
- Providing load file data block signatures according to its own security policy for integrity and source authenticity.

4.2.4 On-Card Components' Security Requirements

4.2.4.1 Runtime Environment Security Requirements

The runtime environment is responsible for:

- Providing an interface to all Applications that ensures that the runtime environment security mechanisms cannot be bypassed, deactivated, corrupted or otherwise circumvented;
- Performing secure memory management to ensure that:

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0044

  - Each application's code and data (including transient session data) as well as the runtime environment itself and its data (including transient session data) is protected from unauthorized access from within the card;
  - When more than one logical channel is supported, each concurrently selected Application's code and data (including transient session data) as well as the runtime environment itself and its data (including transient session data) is protected from unauthorized access from within the card;
  - The previous contents of the memory is not accessible when that memory is reused;
  - The memory recovery process is secure and consistent in case of a loss of power or withdrawal of the card from the card reader while an operation is in progress;
- Providing communication services with off-card entities that ensures the proper transmission (according to the specific communication protocol rules) of unaltered command and response messages.

(See the appropriate runtime environment documentation for more details).

4.2.4.2 Trusted Framework Requirements

Each Trusted Framework present on the card shall:

- Check the application access rules of the inter-acting Applications according to their respective privileges;
- Enforce the Trusted Framework security rules for inter-application communication, including the rules; defined in appendix G;
- Ensure that incoming messages are properly routed unaltered to their intended destinations;
- Ensure that any response messages are properly returned unaltered (except for any cryptographic protection) to the original receiver of the incoming message.

4.2.4.3 OPEN Security Requirements

The OPEN shall:

- Provide an interface to all Applications that ensures that the GlobalPlatform security mechanism cannot be bypassed, deactivated, corrupted or otherwise circumvented;
- Check application access rules according to the Applications' privileges;
- Manage card and Application Life Cycle (see chapter 5 - *Life Cycle Models*);
- Ensure that the Card Content changes are authorized by the Card Issuer;
- Ensure that application code has been signed by the Controlling Authority represented on the card;
- Ensure that application code has been signed by Application Providers represented on the card, if required.

4.2.4.4 Security Domain Security Requirements

Security Domains enforce the security policies of their off-card Security Domain Provider.

When applicable a Security Domain shall:

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0045

- Communicate with off-card entities in accordance with its Security Domain Provider's security policy in Pre-Issuance and Post-Issuance;
- Manage on-card data securely;
- Provide cryptographic protection services for its own Applications during their personalization and optionally during their subsequent operation;
- Request the OPEN to load, install, extradite, and delete card content;
- Return to the off-card entity any receipt for load, install, extradition, and delete;
- Verify the authorization for Card Content changes initiated by an off-card authority;
- Generate receipts for load, install, extradition, and delete;
- Verify the load file data block signature when requested by the OPEN.

4.2.4.5 Global Services Application Security Requirements

A Global Services Application shall:

- Be able to provide services to other Applications, such as CVM services;
- Hold the Global Services application-related data securely;
- Perform internal security measures as required by the service.

4.2.4.6 Application Security Requirements

Applications should:

- Expose only data and resources that are necessary for proper application functionality and;
- Perform internal security measures required by the Application Provider.

4.2.5 Back-End System Security Requirements

Despite the best efforts of the card and the loading processes to provide a stable and secure environment, these components alone cannot ensure total security. The back-end systems (multiple back-end systems may exist for a single card), which communicate with the cards, perform the verifications, and manage the off-card key databases, also shall be trusted. Responsible personnel, secure operating systems, system security policies, and audit procedures are all essential components that secure the back-end systems. These requirements are beyond the scope of this Specification. Information on GlobalPlatform's off-card requirements relating to card management can be found in the GlobalPlatform Key Management System Functional Requirements, GlobalPlatform Smart Card Management System Functional Requirements and GlobalPlatform Messaging Specification.

4.3 Cryptographic support

One of the major requirements for a GlobalPlatform card is the ability to provide a minimum level of cryptographic functionality. This cryptography is, for example, used for the generation of signatures, and is available for use by the Applications present on the card.

The Issuer Security Domain shall implement one Secure Channel Protocol. A Security Domain other than the Issuer Security Domain shall implement [at least] one Secure Channel Protocol. A GlobalPlatform card should support symmetric cryptography such as the Data Encryption Standard (DES) algorithm. A

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0046

GlobalPlatform card may also support asymmetric cryptography such as the Rivest / Shamir / Adleman (RSA) algorithm.

The following cryptographic services are described in this section:

- Integrity and authentication;
- Secure messaging.

When present, services to encrypt and decrypt any pattern of data using these algorithms shall be available to Applications.

It is the responsibility of the Card Issuer or the Controlling Authority to set up the appropriate off-card procedures to comply with the governmental restrictions upon cryptography. Features to disable or restrict cryptography usage by Applications on a card are beyond the scope of this Specification.

4.3.1 Secure Card Content Management

The concepts of integrity and authentication represent an additional value associated with a message or a block of data.

The purpose of this additional value is to provide a method of verifying the source and/or the integrity of particular block of code or data.

The following describes the different usages of integrity and authentication for Card Content management in this Specification.

4.3.1.1 Load File Data Block Hash

The Load File Data Block Hash is intended to verify the integrity of a complete Load File Data Block when loaded to a GlobalPlatform card.

The Load File Data Block Hash is used in the computation of:

- The Load File Data Block Signature (see section 4.3.1.2 - *Load File Data Block Signature*); and
- The Load Token (see section 4.3.1.3 - *Delegated Management Tokens*).

4.3.1.2 Load File Data Block Signature (DAP)

The Load File Data Block Signature is an authentication value generated by an off-card entity (an Application Provider or a Controlling Authority). This is the signature of the Load File Data Block Hash and is included in the DAP Block of the Load File. One or more DAP Blocks may be included in a Load File.

When present during the loading of a Load File to the card, each signature shall be verified by the appropriate Security Domain. The verification operation is referred to as Data Authentication Pattern (DAP) Verification.

4.3.1.3 Delegated Management Tokens

Delegated Management Tokens are signatures of one or more Delegated Management functions (loading, installing, extraditing and deleting) generated by the Card Issuer and used to provide the Card Issuer the control over these Card Content changes. Tokens shall be verified by the appropriate Security Domain.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0047

4.3.1.4 Receipts

The appropriate Security Domain may generate Receipts during Delegated Management. A Receipt is proof that an Application Provider has modified the Card Content.

4.3.2 Secure Communication

A GlobalPlatform card may provide security services related to information exchanged between the card and an off-card entity. The security level of the communication with an off-card entity does not necessarily apply to each individual message being transmitted but can only apply to the environment and/or context in which messages are transmitted. The concept of the Life Cycle of the card (see section 5.1 - *Card Life Cycle*) may be used to determine the security level of the communication between the card and an off-card entity.

The choice of cryptographic algorithms for secure communication is assumed to be industry and product specific.

A GlobalPlatform card offers the following security services associated with messages and defined within a Secure Channel Protocol (see chapter 10 - *Secure Communication*):

- **Entity authentication** - in which the card or the off-card entity proves its authenticity to the other entity through a cryptographic exchange;
- **Integrity and authentication** - in which the receiving entity (the card or off-card entity) ensures that the data being received from the sending entity (respectively the off-card entity or card) actually came from an authenticated entity in the correct sequence and has not been altered;
- **Confidentiality** - in which data being transmitted from the sending entity (the off-card entity or card) to the receiving entity (respectively the card or off-card entity) is not viewable by an unauthenticated entity.

Authentication of the off-card entity combined with the card Life Cycle State allows the card to assume its environment and/or context.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0048

Part III
Implementation

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0049

5 Life Cycle Models

The GlobalPlatform defines Life Cycle models to control the functionality and security of the following GlobalPlatform components:

- Card;
- Executable Load Files;
- Executable Modules;
- Security Domains;
- Applications.

The OPEN owns and maintains the Life Cycle information within the GlobalPlatform Registry and manages the requested state transitions.

The Life Cycle models of each component are presented in this chapter.

5.1 Card Life Cycle

The OPEN is responsible for maintaining the overall security and administration of the card and its content. As the OPEN plays this supervisory role over the entire card, its life cycle can be thought of as the life cycle of the card and is referred to as the card Life Cycle in the subsequent sections.

From a GlobalPlatform perspective, the card Life Cycle begins with the state OP_READY. Although a cards life includes activities prior to the initial card Life Cycle State, these activities are considered card implementation specific and are beyond the scope of this Specification.

The end of the card Life Cycle is the state TERMINATED.

The Issuer Security Domain inherits the card Life Cycle State.

5.1.1 Card Life Cycle States

The following card Life Cycle States shall apply:

- OP_READY
- INITIALIZED
- SECURED
- CARD_LOCKED
- TERMINATED

The card Life Cycle States OP_READY and INITIALIZED are intended for use during the Pre-Issuance phases of the card's life.

The states SECURED, CARD_LOCKED and TERMINATED are intended for use during the Post-Issuance phase of the card although it is possible to terminate the card at any point during its life.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0050

5.1.1.1 Card Life Cycle State OP_READY

The state OP_READY indicates that the runtime environment shall be available and the Issuer Security Domain, acting as the selected Application, shall be ready to receive, execute and respond to APDU commands.

The following functionality shall be present when the card is in the state OP_READY:

- The runtime environment shall be ready for execution;
- The OPEN shall be ready for execution;
- The Issuer Security Domain shall be the implicitly selected Application for all card interfaces;
- Executable Load Files that were included in Immutable Persistent Memory shall be registered in the GlobalPlatform Registry;
- An initial key shall be available within the Issuer Security Domain.

The card shall be capable of Card Content changes, the loading of the Load Files containing applications not already present in the card may occur.

The installation, from Executable Load Files, of any Application may occur.

Additionally, if any personalization information is available at this stage, Applications may be personalized.

The OP_READY state may be used by an off-card entity to perform the following actions:

- Supplementary Security Domains may be loaded and/or installed;
- The Security Domain keys may be inserted in order to maintain a cryptographic key separation from the Issuer Security Domain keys.

5.1.1.2 Card Life Cycle State INITIALIZED

The state INITIALIZED is an administrative card production state. The state transition from OP_READY to INITIALIZED is irreversible. Its functionality is beyond the scope of this Specification. This state may be used to indicate that some initial data has been populated (e.g. Issuer Security Domain keys and/or data) but that the card is not yet ready to be issued to the Cardholder.

5.1.1.3 Card Life Cycle State SECURED

The state SECURED is the intended operating card Life Cycle State in Post-Issuance. This state may be used by Security Domains and Applications to enforce their respective security policies. The state transition from INITIALIZED to SECURED is irreversible.

The SECURED state should be used to indicate to off-card entities that the Issuer Security Domain contains all necessary keys and security elements for full functionality.

5.1.1.4 Card Life Cycle State CARD_LOCKED

The card Life Cycle state CARD_LOCKED is present to provide the capability to disable the selection of Security Domain and Applications. The card Life Cycle state transition from SECURED to CARD_LOCKED is reversible.

Setting the card to this state means that the card shall only allow selection of the application with the Final Application privilege.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0051

Card Content changes including any type of data management (specifically Security Domain keys and data) are not allowed in this state.

Either the OPEN, or a Security Domain with Card Lock privilege, or an Application with Card Lock privilege (see section 6.6 - *Privileges*), may initiate the transition from the state SECURED to the state CARD_LOCKED.

5.1.1.5 Card Life Cycle State TERMINATED

The state TERMINATED signals the end of the card Life Cycle and the card. The state transition from any other state to TERMINATED is irreversible.

The state TERMINATED shall be used to permanently disable all card functionality with respect to any card content management and any life cycle changes. This card state is intended as a mechanism for an Application to logically 'destroy' the card for such reasons as the detection of a severe security threat or expiration of the card. If a Security Domain has the Final Application privilege only the GET DATA command shall be processed, all other commands defined in this specification shall be disabled and shall return an error. If an application has the Final Application privilege its command processing is subject to issuer policy.

The OPEN itself, or a Security Domain with Card Terminate privilege, or an Application with Card Terminate privilege (see section 6.6 - *Privileges*), may initiate the transition from any of the previous states to the state TERMINATED.

5.1.2 Card Life Cycle State Transitions

Figure 5-1 illustrates the state transition diagram for the card Life Cycle. This can typically be viewed as a sequential process with certain possibilities for reversing a state transition or skipping states.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0052

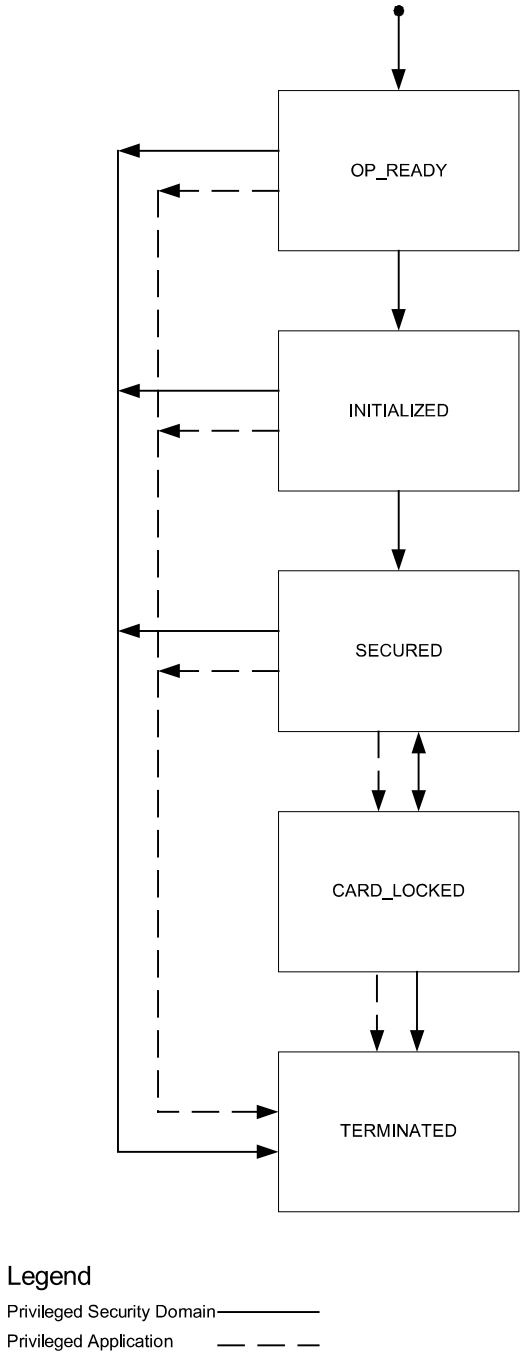


Figure 5-1: Card Life Cycle State Transitions

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0053

5.2 Executable Load File/ Executable Module Life Cycle

An Executable Load File is the actual on-card container of one or more application's executable code (Executable Modules). It may reside in Immutable Persistent Memory or may be created in Mutable Persistent Memory as the resulting image of a Load File Data Block. The format in which the Executable Load File is stored on the card is beyond the scope of this Specification.

The OPEN owns and maintains the Executable Load File Life Cycle information within the GlobalPlatform Registry.

5.2.1 Executable Load File Life Cycle

The Executable Load File Life Cycle can only have one state.

5.2.1.1 Executable Load Life Cycle LOADED

The OPEN shall consider all Executable Load Files present in the card in Immutable Persistent Memory or Mutable Persistent Memory to be in the state LOADED. An Executable Load File transferred to the card through a Load File shall become an entry in the GlobalPlatform Registry following the successful completion of the load process. Executable Load Files present in Immutable Persistent Memory shall automatically have entries within the GlobalPlatform Registry and initially be associated with the Issuer's Security Domain.

5.2.1.2 Executable Load File Deletion

The OPEN may receive a request to delete an Executable Load File. If the Executable Load File cannot be physically deleted (e.g., because it is stored in Immutable Persistent Memory), the following behavior shall apply except that the actual space cannot be reclaimed.

The space previously used to store a physically deleted Executable Load File is reclaimed and may be reused. The entries within the GlobalPlatform Registry of the Executable Load File and each Executable Module within the Executable Load File shall no longer be available, and the OPEN is not required to maintain a record of the deleted Executable Load File's or Executable Module's previous existence.

If the received request is also intended to delete each of the Applications instantiated from the Executable Modules within this Executable Load File, then for each of these Applications the behavior described in section 5.3.1.4 - *Application Deletion* or section 5.3.2.5 - *Security Domain Deletion* shall occur.

5.2.2 Executable Module Life Cycle

The Executable Module Life Cycle is linked to the Executable Load File Life Cycle.

5.3 Application and Security Domain Life Cycle

The Life Cycle of the Application or Security Domain begins when the application is instantiated from an Executable Module. The Life Cycle reflects states that are controlled by the OPEN and states that are controlled directly by the Application.

The Application becomes an entry in the GlobalPlatform Registry and the OPEN sets the Application Life Cycle State to the initial state of INSTALLED during the Application installation process. The OPEN is also responsible for making the Application available for selection by setting its Life Cycle State to SELECTABLE upon request during the Application installation process.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0054

Once an Application or Security Domain is available for selection, it takes control of managing its own Life Cycle. The definition of these state transitions is Application or Security Domain dependent and not controlled by the OPEN.

At any point in the Application or Security Domain Life Cycle, the OPEN may take control for security protection by setting the Life Cycle State to LOCKED. The OPEN also controls the deletion of an Application from the card.

5.3.1 Application Life Cycle States

This Specification defines the following Application Life Cycle States:

INSTALLED

SELECTABLE

LOCKED

In addition to these Application Life Cycle States, the Application may define its own Application dependent states.

Once the Application reaches the SELECTABLE state, it is responsible for managing the next steps of its own Life Cycle. It may use any Application specific states as long as these do not conflict with the states already defined by GlobalPlatform. The OPEN may not perform these transitions without instruction from the Application and the Application is responsible for defining state transitions and ensuring that these transitioning rules are respected.

5.3.1.1 Application Life Cycle State INSTALLED

The state INSTALLED means that the Application executable code has been properly linked and that any necessary memory allocation has taken place. The Application becomes an entry in the GlobalPlatform Registry and this entry is accessible to off-card entities authenticated by the associated Security Domain. The Application is not yet selectable. The installation process is not intended to incorporate personalization of the Application, which may occur as a separate step.

5.3.1.2 Application Life Cycle State SELECTABLE

The state SELECTABLE means that the Application is able to receive commands from off-card entities. The state transition from INSTALLED to SELECTABLE is irreversible. The Application shall be properly installed and functional before it may be set to the state SELECTABLE. The transition to SELECTABLE may be combined with the Application installation process.

The behavior of the Application in the state SELECTABLE is beyond the scope of this Specification.

5.3.1.3 Application Life Cycle State LOCKED

The OPEN, the Application itself, the Application's associated Security Domain, an Application with the Global Lock privilege or a Security Domain with the Global Lock privilege uses the state LOCKED as a security management control to prevent the selection, and therefore the execution, of the Application.

If the OPEN detects a threat from within the card and determines that the threat is associated with a particular Application, that Application may be prevented from further selection by the OPEN setting the state to LOCKED.

Alternatively, the off-card entity may determine that a particular Application on the card needs to be locked for a business or security reason and may initiate the Application Life Cycle transition via the OPEN.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0055

Once the state is LOCKED, only the Application's associated Security Domain, an Application with Global Lock privilege or a Security Domain with Global Lock privilege is allowed to unlock the Application. The OPEN shall ensure that the Application Life Cycle returns to its previous state.

5.3.1.4 Application Deletion

At any point in the Application Life Cycle, the OPEN may receive a request to delete an Application.

The space previously used to store a physically deleted Application is reclaimed and may be reused. The entry within the GlobalPlatform Registry shall no longer be available, and the OPEN is not required to maintain a record of the deleted Application's previous existence.

5.3.1.5 Application Specific Life Cycle States

These states are Application specific. The behavior of the Application, while in these states, is determined by the Application itself and is beyond the scope of this Specification. The OPEN does not enforce any control on Application specific Life Cycle State transitions.

5.3.1.6 Application Life Cycle State Transitions

Figure 5-2 illustrates the state transition diagram for the Application Life Cycle. This can typically be viewed as a sequential process with certain possibilities for reversing a state transition or skipping states.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0056

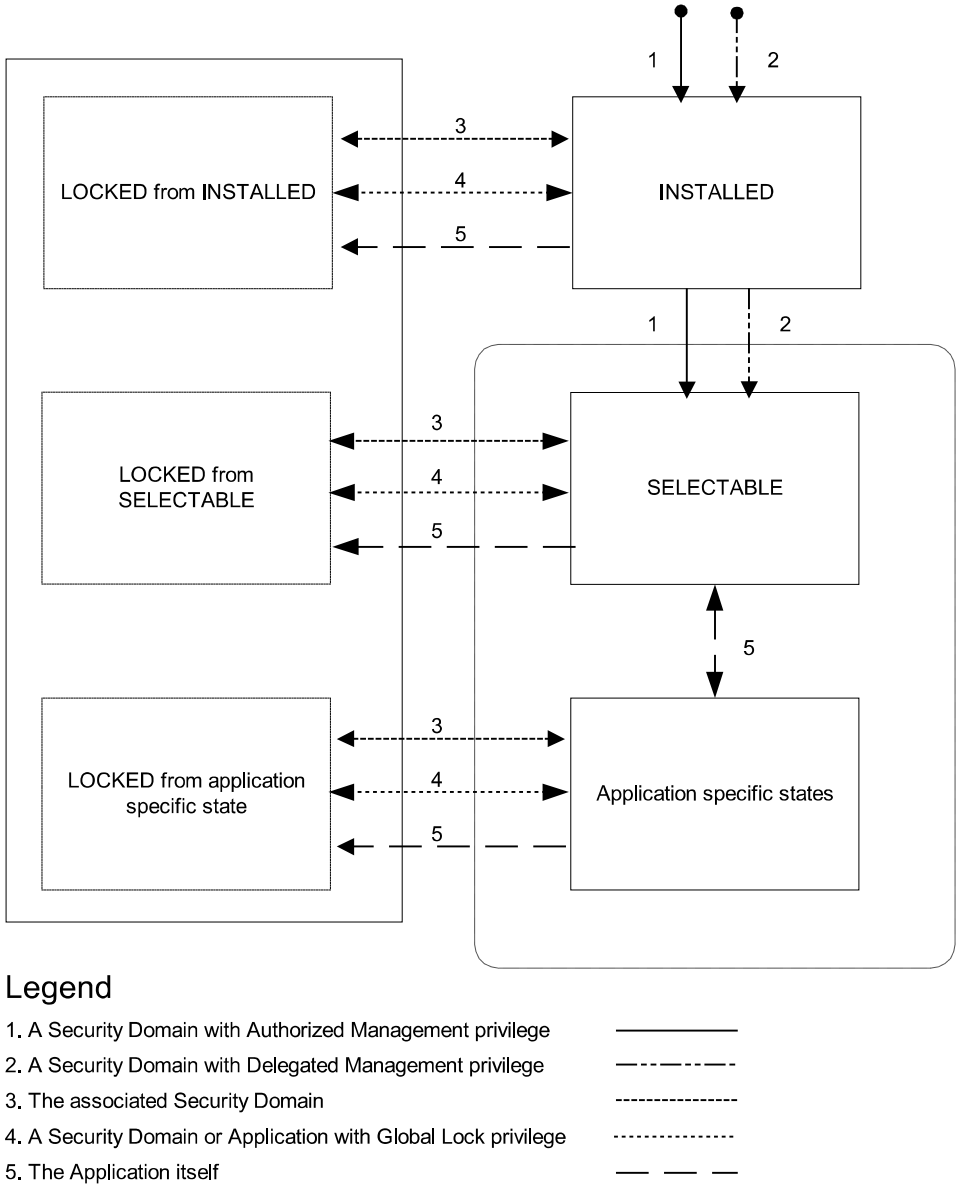


Figure 5-2: Application Life Cycle State Transitions

5.3.2 Security Domain Life Cycle States

This Specification defines the following states applicable to a Security Domain:

1. INSTALLED
2. SELECTABLE
3. PERSONALIZED

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0057

4. LOCKED

There are no proprietary Security Domain Life Cycle States.

5.3.2.1 Security Domain Life Cycle State INSTALLED

The state INSTALLED means that the Security Domain becomes an entry in the GlobalPlatform Registry and this entry is accessible to off-card entities authenticated by the associated Security Domain. The Security Domain is not yet available for selection. It cannot be associated with Executable Load Files or Applications yet and therefore its Security Domain services are not available to Applications.

5.3.2.2 Security Domain Life Cycle State SELECTABLE

The state SELECTABLE means that the Security Domain is able to receive commands (specifically personalization commands) from off-card entities. As they still do not have keys, the Security Domains cannot be associated with Executable Load Files or Applications and therefore their services are not available to Applications when they are in this state. The state transition from INSTALLED to SELECTABLE is irreversible. The transition to SELECTABLE may be combined with the Security Domain installation process.

5.3.2.3 Security Domain Life Cycle State PERSONALIZED

The definition of what is required for a Security Domain to transition to the state PERSONALIZED is Security Domain dependent but is intended to indicate that the Security Domain has all the necessary personalization data and keys for full runtime functionality (i.e. usable in its intended environment). The transition from SELECTABLE to PERSONALIZED (initiated by the Security Domain itself) is irreversible.

In the state PERSONALIZED, the Security Domain may be associated with Applications and its services become available to these associated Applications.

5.3.2.4 Security Domain Life Cycle State LOCKED

The OPEN, the Security Domain itself, the Security Domain's associated Security Domain (if any), an Application with the Global Lock privilege or a Security Domain with the Global Lock privilege uses the state LOCKED as a security management control to prevent the selection of the Security Domain.

If the OPEN detects a threat from within the card and determines that the threat is associated with a particular Security Domain, that Security Domain may be prevented from further selection by the OPEN setting the Security Domain's Life Cycle State to LOCKED.

Alternatively, the off-card entity may determine that a particular Security Domain on the card needs to be locked for a business or security reason and may initiate the state transition via the OPEN.

In this state, the Security Domain is prevented from being used for Delegated Management if applicable. Locking a Security Domain prevents this Security Domain from being associated with new Executable Load Files or Applications. In this state DAP verification, extradition and access to that Security Domain’s services shall fail. In summary, if a Security Domain is in the lifecycle state LOCKED, it shall reject all received commands.

Once the Life Cycle State is LOCKED, only the Security Domain's associated Security Domain (if any), an Application with Global Lock privilege or a Security Domain with Global Lock privilege is allowed to unlock the Security Domain. The OPEN shall ensure that the Security Domain's Life Cycle returns to its previous state.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0058

5.3.2.5 Security Domain Deletion

At any point in the Security Domain Life Cycle, the OPEN may receive a request to delete a Security Domain.

The space previously used to store a physically deleted Security Domain is reclaimed and may be reused. The entry within the GlobalPlatform Registry shall no longer be available, and the OPEN is not required to maintain a record of the deleted Security Domain's previous existence.

5.3.2.6 Security Domain Life Cycle State Transitions

Figure 5-3 illustrates the state transition diagram for the Security Domain Life Cycle. This can typically be viewed as a sequential process with certain possibilities for reversing a state transition or skipping states.

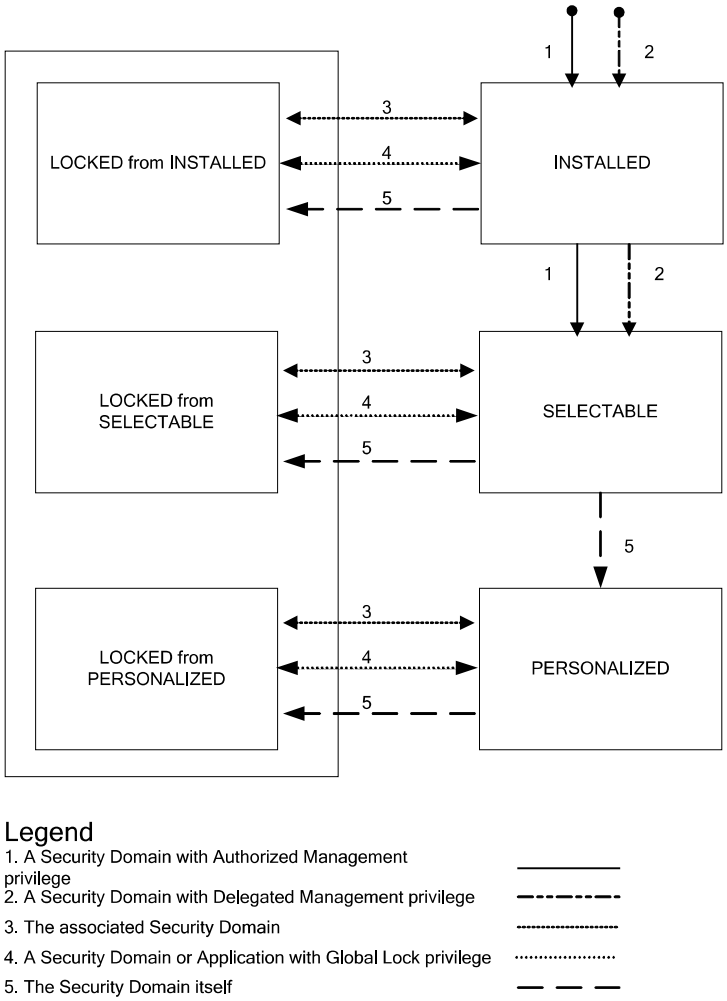


Figure 5-3: Security Domain Life Cycle State Transitions

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0059

5.4 Sample Life Cycle Illustration

This section provides a description of a sample GlobalPlatform card and its Life Cycle transitions from the card's creation to the time it is terminated. It also shows the status of several Executable Load Files, Executable Modules and Applications and their relationship with the card Life Cycle. Figure 5-4 illustrates these sample Life Cycle States:

Application A: Application code is present as an Executable Module within an Executable Load File in Mutable Persistent Memory when the card is manufactured. It is installed in an implementation specific manner. It is used throughout the card's life until the card is terminated and as long as the card is not in a CARD_LOCKED state.

Application B: Application code is present as an Executable Module within an Executable Load File in Immutable Persistent Memory when the chip is manufactured. It is installed prior to the card being initialized. Application B, along with its Executable Load File, is deleted some time during the card's life before the card is terminated. Because the Executable Load File for Application B is stored in Immutable Persistent Memory, it cannot be physically deleted from the card.

Application C: Application code is present as an Executable Module within an Executable Load File and is loaded in an implementation specific manner. The Application is installed in Post-Issuance while the card is in the Life Cycle State SECURED. The Application is used for some time and then deleted along with its Executable Load File before the card is terminated. Because the Application and its Executable Load File are stored in Mutable Persistent Memory, the Application and associated Executable Load File, along with all its Executable Modules, are purged from Mutable Persistent Memory and the memory space reclaimed for reuse.

Application D: Application code is present as an Executable Module within an Executable Load File and is loaded in an implementation specific manner. It is used during the full lifetime of the card until the card is terminated and as long as the card Life Cycle State is not CARD_LOCKED.

Application E: Application code is present as an Executable Module within an Executable Load File that is loaded and installed in Post-Issuance while in the card Life Cycle State SECURED. Application E is used until the card is terminated and as long as the card Life Cycle State is not CARD_LOCKED.

Application F: Application code is present as an Executable Module within the same Executable Load File as Application E. It is loaded and installed in Post-Issuance while in the card Life Cycle State SECURED. Application F is deleted some time during the card's lifetime.

Note that the following diagram is not intended to be a comprehensive description of what is permitted in each card Life Cycle State.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0060

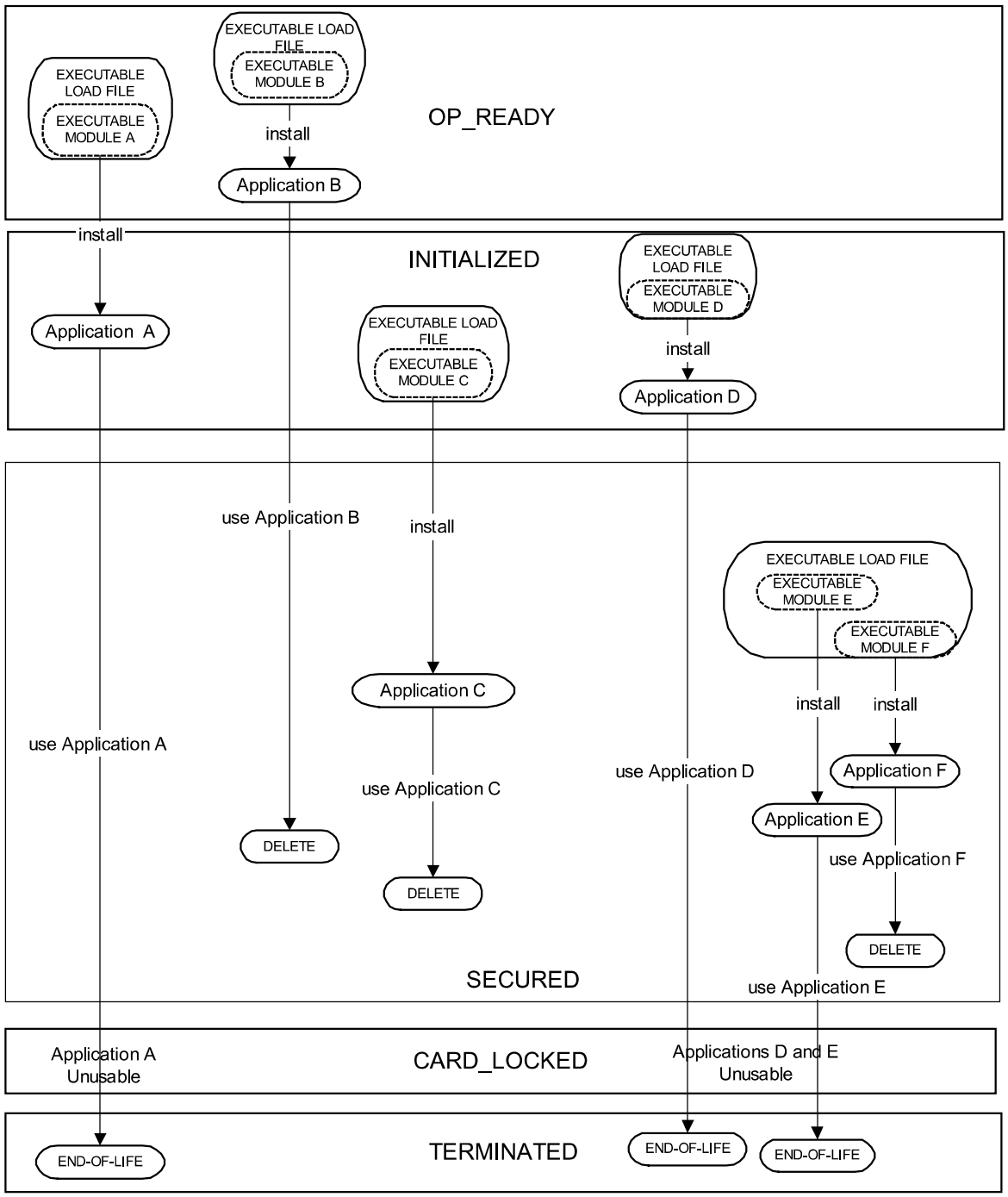


Figure 5-4: Sample Card Life Cycle and Application Life Cycles

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0061

6 GlobalPlatform Environment (OPEN)

6.1 Overview

The GlobalPlatform Environment (OPEN) supports the following functions if the underlying runtime environment does not support them:

- **Command Dispatch**
  - Application and Security Domain selection
  - (Optional) Logical channel management
  - Command dispatching
- **Card Content Management**
  - Content verification
  - Content loading
  - Content installation
  - Content removal
  - Access control rules for card content management
- **Security Management**
  - Security Domain locking and unlocking
  - Application locking and unlocking
  - Card locking and unlocking
  - Card termination
  - Privilege usage
  - Security Domain privilege usage
  - Tracing and event logging
- **GlobalPlatform Trusted Framework**
  - Secure inter-application communication

The OPEN architecture may be illustrated as a collection of system functions built upon a GlobalPlatform Registry. The GlobalPlatform Registry is a data store required to support the various system functions of the GlobalPlatform.

The following are some examples of the use of the GlobalPlatform Registry by the OPEN.

Command Dispatch:

- Determine if an Application or Security Domain is present and available to respond to a SELECT command;
- When supported, manage logical channels;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0062

- Dispatch commands to the selected Application for command processing.

Card Content Management:

- Store state and management information about newly loaded Executable Load Files, Executable Modules, and installed Applications;
- Store the Security Domain to be associated with Executable Load Files being loaded;
- Store the privileges and associated Security Domains of the Applications being installed;
- Identify an Application's associated Security Domain to provide access for that Application to its Security Domain services.

Security Management:

- Allow the audit of Card Content by retrieving status information related to any Application present on the card;
- Verify the integrity and request verification of the authenticity for Executable Load Files;
- Verify that resource restrictions are respected during loading and installing of new content and during Application runtime execution;
- Verify an Application's or a Security Domain's accessibility to functionality that requires privileges.

6.2 OPEN Services

Appendix A.1 - *GlobalPlatform on a Java Card* provides the Java Card™ implementation of the following interfaces.

Appendix A.2 - *GlobalPlatform on MULTOS*™ provides the MULTOS™ implementation of the following interfaces.

Applications and Security Domains may access and/or modify some content known or managed by the OPEN. Depending on the relevant privileges of the requesting entity, the following services shall be provided by the OPEN:

- Retrieving the Application's own Life Cycle State stored by the OPEN in the GlobalPlatform Registry;
- Retrieving the card Life Cycle State;
- Obtaining access to the services of the Security Domain associated with the Application;
- Transitioning the card Life Cycle State to CARD_LOCKED;
- For contact cards according to ISO/IEC 7816-4 and for contactless cards Type A according to ISO/IEC 14443-3, setting the content of the historical bytes;
- Transitioning the Application's own Application Life Cycle State stored by the OPEN in the GlobalPlatform Registry;
- Transitioning the card Life Cycle State to TERMINATED;
- Obtaining access to GlobalPlatform Registry information;
- Obtaining access to Global Services Applications.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0063

6.3 Command Dispatch

The commands received by a GlobalPlatform card shall be processed by the OPEN or dispatched to the selected Application for processing.

The SELECT [by name] command is processed by the OPEN.

One option of making the Issuer Security Domain the selected Application, is to specify its AID in a SELECT command with the [first or only occurrence] option set. As another option for making the Issuer Security Domain the selected Application, the SELECT command could contain no data in which case the AID of the Issuer Security Domain would be discovered by the off-card entity in the response to the SELECT command.

The processing of the MANAGE CHANNEL command is dependent on the capabilities of the card:

- If the card is aware of logical channels but only supports the Basic Logical Channel, the OPEN shall respond with the appropriate error;
- If the card is aware of logical channels and supports at least one Supplementary Logical Channel, the OPEN shall process the command; or
- If the card only supports the Basic Logical Channel and has no concept of logical channel support, the command shall be dispatched to the selected Application for processing.

Any other type of command received shall be dispatched to the currently selected Application.

Commands are either received on the Basic Logical Channel (logical channel number zero) or on a Supplementary Logical Channel (logical channel number other than zero). In compliance with ISO/IEC 7816-4, logical channel information shall be indicated in the class byte of the APDU command header. For all commands, if the command indicates a Supplementary Logical Channel that is not opened then:

- If the card only supports the Basic Logical Channel and has no concept of logical channel support, the command shall be dispatched to the selected Application for processing.
- If the card is aware of logical channels, the OPEN shall respond with the appropriate error. (This requirement may exclude the SELECT command, if the card supports opening of a logical channel using the SELECT command.)

For commands that are dispatched to an Application, it is the responsibility of the Application to correctly reject commands that it does not recognize, expect or cannot process.

The way in which an Application exhibits its multi-selection capabilities can vary according to the underlying platform and is beyond the scope of this Specification.

The Issuer Security Domain shall have no multi-selection restrictions on cards that support multiple logical channels i.e. it shall be capable of being selected across multiple logical channels.

6.4 Logical Channels and Application Selection

6.4.1 Implicit Selection Assignment

The following rules apply to the assignment of implicit selection to an Application:

- The Issuer Security Domain is by default the implicitly selectable Application on all logical channels of all card I/O interfaces supported by the card. Implicit selection on a specific logical channel of a specific card I/O interface may be assigned only if the Issuer Security Domain is the implicitly selectable Application on that logical channel of that card I/O interface and no other Locked Application is registered as implicitly selectable for the same logical channel and card I/O interface (see 9.6.2 - *Application Locking and Unlocking*;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0064

- An Application installed or made selectable with a specific Implicit Selection parameter is registered in the GlobalPlatform Registry as the implicitly selectable Application on the logical channel(s) of the card I/O interface(s) indicated in the parameter if no other Application (other than the Issuer Security Domain) is already registered as implicitly selectable on that logical channel(s) of that card I/O interface(s);
- An Application installed or made selectable with the Card Reset privilege and no Implicit Selection parameter is registered in the GlobalPlatform Registry as the implicitly selectable Application on the Basic Logical Channel for all card I/O interfaces supported by the card if no other Application (other than the Issuer Security Domain) is already registered as implicitly selectable on the Basic Logical Channel of any card I/O interface;
- If an Application implicitly selectable on specific logical channel(s) of specific card I/O interface(s) is deleted, the Issuer Security Domain becomes the implicitly selectable Application on that logical channel(s) of that card I/O interface(s).

The OPEN shall use the implicit selection registration of each Application for controlling the following runtime behavioral requirements:

- Identifying the Application which is implicitly selectable on the Basic Logical Channel of the current card I/O interface during the card reset or activation sequence;
- Identifying the Application which is implicitly selectable when opening on the current card I/O interface a new Supplementary Logical Channel from the Basic Logical Channel.

6.4.2 Basic Logical Channel

The Basic Logical Channel is the permanently available interface to a GlobalPlatform card. This Basic Logical Channel shall be supported by the OPEN.

6.4.2.1 Application Selection on Basic Logical Channel

The OPEN shall support Application selection on the Basic Logical Channel via two processes:

- Implicit Selection following the card reset (see ISO/IEC 7816-3 for contact cards) or activation sequence (see ISO/IEC 14443-3 for contactless cards);
- Explicit Selection through the SELECT [by name] command.

The OPEN may also support additional selection processes.

Partial AID selection as defined in section 6.4.2.1.2 - *Explicit Selection*, shall be supported. (Partial AID selection does not require knowledge of the full AID by the off-card entity.) As multiple Applications on the card may have the same partial AID, it is required that a method exists to select all Applications matching the partial AID.

6.4.2.1.1 Implicit Selection on Basic Logical Channel

Once the card session has been established (for contact cards according to ISO/IEC 7816-4 after Answer-to-Reset, or after the activation sequence for contactless cards according to ISO/IEC 14443-3), and before the first command is issued to the card, the Application defined as implicitly selectable on the Basic Logical Channel and for that card I/O interface shall become the selected Application on the Basic Logical Channel for that card I/O interface.

Runtime Behavior

The following requirements apply for the OPEN for the implicit Application selection process:

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0065

- If the card is in the Life Cycle State CARD_LOCKED or TERMINATED, the Application with the Final Application privilege is the selected Application on the Basic Logical Channel and the OPEN shall not attempt to identify the implicitly selectable Application;
- In all other cases the OPEN shall search the GlobalPlatform Registry for an Application that is marked as implicitly selectable on the Basic Logical Channel for the current card I/O interface (e.g. contact or contactless), and if this Application is not in the Life Cycle State LOCKED, it shall become the selected Application on the Basic Logical Channel. If this is an Application in the Life Cycle State LOCKED, the Application with the Final Application privilege shall become the selected Application on the Basic Logical Channel.

6.4.2.1.2 Explicit Selection on Basic Logical Channel

At any time during a Card Session the OPEN may receive a request to select an Application on the Basic Logical Channel (SELECT [by name] [first or only occurrence] command). The OPEN shall determine if the requested AID matches or partially matches an entry within the GlobalPlatform Registry and whether this entry is selectable.

At any time during a Card Session that has already contained a SELECT [by name] [first or only occurrence] command, the OPEN may receive a request to select a next Application (SELECT [by name] [next occurrence] command) on the Basic Logical Channel. The OPEN shall determine if the requested AID matches or partially matches another entry within the GlobalPlatform Registry and whether this entry is selectable.

For both the SELECT [by name] [first or only occurrence] command and the SELECT [by name] [next occurrence] command, an Application becomes the selected Application on the Basic Logical Channel if:

- The requested AID matches (fully or partially) the Application's AID;
- The Application being selected is in the correct Life Cycle State;
- The Application has no restrictions due to multi-selection, and supports the current card interface.

Runtime Behavior

The following requirements apply to the OPEN in the explicit Application selection (SELECT [by name]) process on the Basic Logical Channel (This behavior does not apply if the card Life Cycle State is TERMINATED):

- In the card Life Cycle State CARD_LOCKED:
  - If the Application being selected has the Final Application privilege, this Application is re-selected and a warning is returned to the off-card entity;
  - If any other Application is being selected, the Application with the Final Application privilege remains selected and an error is returned to the off- card entity;
- If a SELECT [by name] [first or only occurrence] or SELECT [by name] [next occurrence] is received and the data field of the command message is not present, the Issuer Security Domain shall become the currently selected Application and the SELECT command is dispatched to the Issuer Security Domain;
- If a SELECT [by name] [first or only occurrence] is received, the search always begins from the start of the GlobalPlatform Registry;
- If a SELECT [by name] [next occurrence] is received, the search always begins from the entry following the currently selected Application on the Basic Logical Channel in the GlobalPlatform Registry;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0066

- If a full or partial match is found and this Application is in the Life Cycle State INSTALLED, continue searching through the GlobalPlatform Registry for a subsequent full or partial match. If no subsequent full or partial match is found, the OPEN shall return the appropriate error to the off-card entity;
- If a full or partial match is found and this Application is in the Life Cycle State LOCKED, continue searching through the GlobalPlatform Registry for a subsequent full or partial match. In the eventuality that this locked Application is already currently selected on the Basic Logical Channel, the OPEN shall terminate this Application Session. If no subsequent full or partial match is found, the OPEN shall return the appropriate error to the off-card entity;
- If a full or partial match is found and this Application cannot be selected due to a multi-selection restriction or because the Application refuses selection (e.g. because it does not support the current card interface), continue searching through the GlobalPlatform Registry for a subsequent full or partial match. If no subsequent full or partial match is found, the OPEN shall return the appropriate error to the off-card entity;
- If a full or partial match is found and this Application is selectable (i.e. in the correct Life Cycle State and has no multi-selection restrictions), then it shall become the currently selected Application on the Basic Logical Channel and the SELECT [by name] command, whether [first or only occurrence] or [next occurrence], shall be processed according to the requirements of the runtime environment (e.g. dispatched to the Application);
- If no full or partial match is found at all, the currently selected Application on the Basic Logical Channel shall remain the selected Application and
  - If the SELECT [by name] command has the [first or only occurrence] parameter set, the SELECT command is dispatched to the Application;
  - If the SELECT [by name] command has the [next occurrence] parameter set, the OPEN shall return the appropriate error to the off-card entity;
- In the eventuality that the current Application Session has been terminated and no subsequent full or partial match is found, the OPEN shall make an attempt to select the Application that is marked as implicitly selectable on the Basic Logical Channel for the current card interface.

6.4.2.2 Logical Channel Management on Basic Logical Channel

At any time during a Card Session the OPEN may receive a request on the Basic Logical Channel to either open or close a Supplementary Logical Channel.

If the card only supports the Basic Logical Channel and has no concept of logical channel support, the MANAGE CHANNEL command is dispatched to the currently selected Application. In this case, when a Security Domain is the currently selected Application, the command shall be rejected.

On cards that support logical channels, if a MANAGE CHANNEL [open] is received:

- If an Application is designated as implicitly selectable on the new Supplementary Logical Channel for the current card interface, that Application is implicitly selected on the newly opened Supplementary Logical Channel and runtime behavior requirements apply;
- Otherwise the Application designated as implicitly selectable on the Basic Logical Channel for this card interface is implicitly selected on the newly opened Supplementary Logical Channel and runtime behavior requirements apply.

On cards that support logical channels, if a MANAGE CHANNEL [close] is received, terminate the Application Session currently selected on the Supplementary Logical Channel indicated by the command and then close that logical channel. The Basic Logical Channel can never be closed.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0067

Runtime Behavior

On receipt of a MANAGE CHANNEL [open] command, the following requirements apply:

- If the card is in the Life Cycle State CARD_LOCKED or TERMINATED, return the appropriate error.
- If the number of logical channels supported by the OPEN is not sufficient to open a new Supplementary Logical Channel, return the appropriate error.
- The OPEN shall search the GlobalPlatform Registry for the Application that supports the current card interface and that is marked as implicitly selectable on the new Supplementary Logical Channel (or failing that, on the Basic Logical Channel) and:
  - If this is an Application in the Life Cycle State LOCKED, the Application with the Final Application privilege shall become the selected Application on the Supplementary Logical Channel;
  - If this Application cannot be selected due to a multi-selection restriction, the new logical channel shall not be opened and the OPEN shall return the appropriate error;
  - Otherwise, the Supplementary Logical Channel is opened and this Application shall become the selected Application on the Supplementary Logical Channel.

6.4.2.3 Application Command Dispatch on Basic Logical Channel

Once an Application becomes the selected Application on the Basic Logical Channel, the responsibility for subsequent command dispatching still rests with the OPEN.

Processing SELECT [by name] commands and runtime behavior requirements for OPEN are described in section 6.4.2.1.2 - *Explicit Selection*.

On cards that are aware of logical channels, the MANAGE CHANNEL commands are only processed by the OPEN and are not dispatched to an Application.

All other commands (including the MANAGE CHANNEL commands on cards that are not aware of logical channels or SELECT commands not described in section 6.4.2.1.2 - *Explicit Selection*) are immediately dispatched to the Application currently selected on the Basic Logical Channel. The processing of the command by the Application is beyond the scope of this Specification.

6.4.3 Supplementary Logical Channel

A Supplementary Logical Channel, if supported, allows an Application to be selected simultaneously to the Applications selected on other logical channels.

6.4.3.1 Application Selection on Supplementary Logical Channel

The OPEN shall support Application selection on an available Supplementary Logical Channel via two processes:

- Implicit Selection following a successful MANAGE CHANNEL [open] command;
- Explicit Selection through the SELECT [by name] command.

The OPEN may also support additional selection processes.

Partial AID selection as defined in section 6.4.3.1.2 - *Explicit Selection*, shall be supported on Supplementary Logical Channels.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0068

6.4.3.1.1 Implicit Selection on Supplementary Logical Channel

Depending on whether a Supplementary Logical Channel is being opened from the Basic Logical Channel or from another Supplementary Logical Channel, the behavior of implicit selection differs.

Refer to section 6.4.2.2 - *Logical Channel Management* for the behavior of implicit selection initiated from the Basic Logical Channel.

Refer to section 6.4.3.2 - *Logical Channel Management* for the behavior of implicit selection initiated from a Supplementary Logical Channel.

6.4.3.1.2 Explicit Selection on Supplementary Logical Channel

At any time on an open Supplementary Logical Channel, the OPEN may receive a request to select an Application on this Supplementary Logical Channel (SELECT [by name] [first or only occurrence] command). The OPEN shall determine if the requested AID matches or partially matches an entry within the GlobalPlatform Registry and whether this entry is selectable.

At any time on an open Supplementary Logical Channel that has already contained a SELECT [by name] [first or only occurrence] command since the Supplementary Logical Channel was last opened, the OPEN may receive a request to select a next Application (SELECT [by name] [next occurrence] command) on this Supplementary Logical Channel. The OPEN shall determine if the requested AID matches or partially matches another entry within the GlobalPlatform Registry and whether this entry is selectable.

For both the SELECT [by name] [first or only occurrence] command and the SELECT [by name] [next occurrence] command, an Application becomes the selected Application on the Supplementary Logical Channel if:

- The requested AID matches (fully or partially) the Application's AID;
- The Application being selected is in the correct Life Cycle State;
- The Application has no restrictions due to multi-selection, and supports the current card interface.

Runtime Behavior

The following requirements apply to the OPEN in the explicit Application selection (SELECT [by name]) process on a Supplementary Logical Channel:

- If the card is in the Life Cycle State CARD_LOCKED or TERMINATED:
  - Close the Supplementary Logical Channel, if currently open;
  - Return the appropriate error;
- If a SELECT [by name] [first or only occurrence] or SELECT [by name] [next occurrence] is received and the data field of the command message is not present, the Issuer Security Domain shall become the currently selected Application and the SELECT command is dispatched to the Issuer Security Domain;
- If a SELECT [by name] [first or only occurrence] is received, the search always begins from the start of the GlobalPlatform Registry;
- If a SELECT [by name] [next occurrence] is received, the search always begins from the entry following the currently selected Application on this Supplementary Logical Channel in the GlobalPlatform Registry;
- If a full or partial match is found and this Application is in the Life Cycle State INSTALLED, continue searching through the GlobalPlatform Registry for a subsequent full or partial match. If

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0069

no subsequent full or partial match is found, the OPEN shall return the appropriate error to the off-card entity;

- If a full or partial match is found and this Application is in the Life Cycle State LOCKED, continue searching through the GlobalPlatform Registry for a subsequent full or partial match. In the eventuality that this locked Application is already currently selected on the same Supplementary Logical Channel, the OPEN shall terminate this Application Session. If no subsequent full or partial match is found, the OPEN shall return the appropriate error to the off-card entity;
- If a full or partial match is found and this Application cannot be selected due to a multi-selection restriction or because the Application refuses selection (e.g. because it does not support the current card interface), continue searching through the GlobalPlatform Registry for a subsequent full or partial match. If no subsequent full or partial match is found, the OPEN shall return the appropriate error to the off-card entity;
- If a full or partial match is found and this Application is selectable (i.e. in the correct Life Cycle State and has no multi-selection restrictions), then it shall become the currently selected Application on this Supplementary Logical Channel and the SELECT [by name] command, whether [first or only occurrence] or [next occurrence], shall be processed according to the requirements of the runtime environment (e.g. dispatched to the Application);
- If no full or partial match is found at all, the currently selected Application on the Supplementary Logical Channel shall remain the selected Application and
  - If the SELECT [by name] command has the [first or only occurrence] parameter set, the SELECT command is dispatched to the Application;
  - If the SELECT [by name] command has the [next occurrence] parameter set, the OPEN shall return the appropriate error to the off-card entity.

6.4.3.2 Logical Channel Management on Supplementary Logical Channel

At any time on an open Supplementary Logical Channel the OPEN may receive a request to either open or close a Supplementary Logical Channel.

If a MANAGE CHANNEL [open] is received and the Application selected on the original Supplementary Logical Channel has no multi-selection restrictions, this Application becomes the selected Application on the newly opened Supplementary Logical Channel.

If a MANAGE CHANNEL [close] is received, terminate the Application Session currently selected on the Supplementary Logical Channel indicated by the command and then close that logical channel. The Basic Logical Channel can never be closed.

Runtime Behavior

On receipt of a MANAGE CHANNEL [open] command, the following requirements apply:

- If the card is in the Life Cycle State CARD_LOCKED or TERMINATED, return the appropriate error;
- If the number of logical channels supported by the OPEN is not sufficient to open a new Supplementary Logical Channel, return the appropriate error;
- If the Application currently selected on the original Supplementary Logical Channel cannot be selected on the new Supplementary Logical Channel due to a multi-selection restriction, the new logical channel shall not be opened and the OPEN shall return the appropriate error;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0070

- Otherwise, the Supplementary Logical Channel indicated by the command is opened and the Application currently selected on the original Supplementary Logical Channel shall become the selected Application on the newly opened Supplementary Logical Channel.

6.4.3.3 Application Command Dispatch on Supplementary Logical Channel

Once an Application becomes the selected Application on a Supplementary Logical Channel, the responsibility for subsequent command dispatching still rests with the OPEN.

Processing SELECT [by name] commands and runtime behavior requirements for OPEN are described in section 6.4.3.1.2 - *Explicit Selection*.

The MANAGE CHANNEL commands are only processed by the OPEN and are not dispatched to an Application.

All other commands (including SELECT commands not described in section 6.4.3.1.2 - *Explicit Selection*) are immediately dispatched to the Application currently selected on the Supplementary Logical Channel. The processing of the command by the Application is beyond the scope of this Specification.

6.5 GlobalPlatform Registry

The GlobalPlatform Registry is used to:

- Store card management information;
- Store relevant application management information (e.g., AID, associated Security Domain and Privileges);
- Support card resource management data;
- Store Application Life Cycle information;
- Store card Life Cycle information;
- Track any counters associated with logs.

The contents of the GlobalPlatform Registry may be updated in response to:

- An internal OPEN invoked action;
- An authorized Application invoked action.

All Applications including all Security Domains, and all Executable Load Files, shall have an entry in the GlobalPlatform Registry.

There is no mandatory format for the storage of these data elements. However, format requirements do exist for the handling of the data elements via APDU commands and GlobalPlatform services available to Applications.

6.5.1 Application/Executable Load File/Executable Module Data Elements

6.5.1.1 Application/Executable Load File/Executable Module AID

Each Executable Load File or Executable Module is associated with an AID that shall be unique on the card.

An Application AID may be the same as that of an Executable Module but may not be the same as that of an Executable Load File or the same as another Application already present in the GlobalPlatform Registry.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0071

This AID may be specified in a SELECT command to select the Application. It is not possible to select Executable Load Files or Executable Modules.

6.5.1.2 Application/Executable Load File/Executable Module Life Cycle

The Application Life Cycle State data element contains the current Life Cycle of the Application, Executable Load File or Executable Module.

6.5.1.3 Memory Resource Management Parameters

Resource management data elements contain information about the memory resources that are available to an Application. They are system-specific values and are used as a control mechanism by the OPEN to manage memory resource allocation as described in section 9.7 - *Memory Resource Management*.

When additional resources are requested by an Application, the OPEN shall validate the request against the value of this data element in the GlobalPlatform Registry.

6.5.1.4 Privileges

The Privileges data element indicates the privileges for each Application. Privileges are defined in section 6.6.

6.5.1.5 Implicit Selection Parameter

The implicit selection parameter indicates whether an Application is implicitly selectable on a specific logical channel of a specific card interface: see section 11.1.7 and Table 11-50.

6.5.1.6 Associated Security Domain AID

All Executable Load Files and Applications, including Security Domains, are associated with a Security Domain, whose AID is given in the registry. This AID is the AID of the Security Domain directly associated. A Security Domain also has an associated Security Domain: either another Security Domain or itself, hence describing an association hierarchy of Executable Load Files / Applications and Security Domains.

6.5.1.7 Application Provider ID

The Registry holds the identifier of the Application Provider: the owner of the Application or Executable Load File when explicitly provided during the load or installation process.

An on-card entity may use this information to enforce security policies. Establishing whether an off-card entity is also the owner of the on-card entity being managed is addressed in more detail in section 10.4 - *Entity Authentication*.

6.5.1.8 Service Parameter

A Service Parameter identifies the service offered by the Global Services Application. The Global Services Application may register this service as a unique Global Service as described in section 8.1.1 - *Registering Global Services*. More than one service, hence more than one Service Parameter, may be registered for a Global Services Application.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0072

6.5.2 Card-Wide Data

The card Life Cycle State is stored in the GlobalPlatform Registry similarly to Application information. Any restriction of the Card Content Management functionality of OPEN is stored in the GlobalPlatform Registry.

6.6 Privileges

6.6.1 Privilege Definition

The following table defines Security Domain and Application privileges:

Privilege Number	Privilege	Description	Notes
0	Security Domain	Application is a Security Domain.	Distinguishes a Security Domain from a 'normal' Application.
1	DAP Verification	Application is capable of verifying a DAP; Security Domain privilege shall also be set.	For details, see section 9.2.1.
2	Delegated Management	Application is capable of Delegated Card Content Management: Security Domain privilege shall also be set.	For details, see section 9.1.3.3.
3	Card Lock	Application has the privilege to lock the card.	For details, see section 9.6.3.
4	Card Terminate	Application has the privilege to terminate the card.	For details, see section 9.6.4.
5	Card Reset	Application has the privilege to modify historical bytes on one or more card interfaces. This privilege was previously labeled "Default Selected".	For details, see section 6.6.2.
6	CVM Management	Application has the privilege to manage a shared CVM of a CVM Application.	For details, see section 8.2.1.
7	Mandated DAP Verification	Application is capable of and requires the verification of a DAP for all load operations: Security Domain privilege and DAP Verification privilege shall also be set.	For details, see section 9.2.1.
8	Trusted Path	Application is a Trusted Path for inter-application communication.	For details, see section 6.7.
9	Authorized Management	Application is capable of Card Content Management; Security Domain privilege shall also be set.	For details, see section 9.1.3.2.
10	Token Verification	Application is capable of verifying a token for Delegated Card Content Management.	For details, see sections 9.1.3.1 and 9.2.3.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0073

Privilege Number	Privilege	Description	Notes
11	Global Delete	Application may delete any Card Content.	For details, see sections 9.1.3.4 and 9.5.
12	Global Lock	Application may lock or unlock any Application.	For details, see section 9.1.3.5 and 9.6.2.
13	Global Registry	Application may access any entry in the GlobalPlatform Registry.	For details, see section 9.6.5.
14	Final Application	The only Application accessible in card Life Cycle State CARD_LOCKED and TERMINATED.	For details, see section 9.6.4.
15	Global Service	Application provides services to other Applications on the card.	For details, see section 8.1.1.
16	Receipt Generation	Application is capable of generating a receipt for Delegated Card Content Management.	For details, see section 9.1.3.6
17	Ciphered Load File Data Block	The Security Domain requires that the Load File being associated to it is to be loaded ciphered.	For details, see section 9.1.3.7
18	Contactless Activation	Application is capable of activating and deactivating other Applications on the contactless interface.	For details, see section 7.1 of Amendment C
19	Contactless Self-Activation	Application is capable of activating itself on the contactless interface without a prior request to the Application with the Contactless Activation privilege.	For details, see section 7.2 of Amendment C

Table 6-1: Privileges

6.6.2 Privilege Assignment

The following rules apply to the assignment of Privileges:

- Only one Application or Security Domain in the card may be set with the Card Reset privilege at a time (e.g. the Issuer Security Domain, a current legacy Application or an Application that requires specific behavior with regards to logical channels) on a given card interface;
- Once the Card Reset privilege has been assigned to an Application for a given card interface, the privilege can be reassigned to a new Application either by deleting the Application which has the privilege, or by revoking its privilege;
- The Card Reset privilege is by default assigned to the Issuer Security Domain. It may be reassigned only if the Issuer Security Domain has the Card Reset privilege;
- If the application with the Card Reset privilege is deleted, the privilege is reassigned to the Issuer Security Domain;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0074

- The Final Application privilege is by default assigned to the Issuer Security Domain. It may be reassigned only if the Issuer Security Domain has the Final Application privilege;
- Only one Application or Security Domain in the card may be set with the Final Application privilege at a time (e.g. the Issuer Security Domain, a current legacy Application or an Application that requires specific behavior with regards to logical channels);
- Once the Final Application privilege has been assigned to an Application, the privilege can be reassigned to a new Application either by deleting the Application which has the privilege, or by revoking its privilege;
- If the application with the Final Application privilege is deleted, the Issuer Security Domain becomes the Application with Final Application privilege;
- Authorized Management and Delegated Management privileges are mutually exclusive;
- Token Verification and Delegated Management privileges are mutually exclusive;
- Receipt Generation and Delegated Management privileges are mutually exclusive;
- Otherwise, the privileges are not mutually exclusive; therefore, one or more privileges may be marked as set for an Application.

In the OP_READY card Life Cycle State, the Issuer Security Domain shall initially have the following set of privileges clearly identifying its functionality: Security Domain, Authorized Management, Global Registry, Global Lock, Global Delete, Token Verification, Card Lock, Card Terminate, Trusted Path, CVM Management, Card Reset, Final Application and Receipt Generation.

Privileges may be added or revoked during the Life Cycle of an Application or Security Domain.

For backward compatibility, where a card supports only privileges 0-7, the following assumptions shall apply for the remaining privileges:

Privilege Number	Privilege	Issuer Security Domain	Supplementary Security Domain	Other Application
8	Trusted Path	yes	yes	no
9	Authorized Management	yes	no	no
10	Token Verification	yes	no	no
11	Global Delete	yes	no	no
12	Global Lock	yes	no	no
13	Global Registry	yes	no	no
14	Final Application	yes	no	no
15	Global Service	no	no	no
16	Receipt Generation	yes	no	no
17	Ciphered Load File Data Block	no	no	no
18	Contactless Activation	no	no	no
19	Contactless Self-Activation	no	no	no

Table 6-2: Privilege Defaults

Several use cases can be envisaged for the assignment of privileges to Security Domains, depending on the business relationships between the Card Issuer and other off-card entities: Application Providers or Controlling Authority. The following table shows four example use cases.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0075

		Use case			
		A	B	C	D
Issuer Security Domain	Authorized Management Privilege	✓	✓	✓	
	Delegated Management Privilege				✓
	Token Verification Privilege	✓	✓		✓
	Receipt Generation Privilege	✓	✓		✓
Supplementary Security Domain	Authorized Management Privilege				
	Delegated Management Privilege		✓		✓
	Token Verification Privilege			✓	
	Receipt Generation Privilege			✓	

Table 6-3: Privilege Assignment Example Use Cases

6.6.3 Privilege Management

Runtime Behavior

The OPEN shall use the Privileges data element in conjunction with the association hierarchy (see section 7.2 - *Security Domain Association*) of the Applications for controlling the following runtime behavioral requirements:

- Ensuring Token verification when required (see section 9.3.2 - *Card Content Loading*);
- Ensuring Receipt generation when required (see section 9.3.2 - *Card Content Loading*);
- Ensuring DAP verification when required (see section 9.3.2 - *Card Content Loading*);
- Checking for the validity of a request to change Card Contents: load, installation, extradition, registry update, or deletion;
- Checking for the validity of a request to lock or unlock the card;
- Checking for the validity of a request to lock or unlock an Application, including a Security Domain;
- Checking for the validity of a request to terminate the card;
- Checking for the validity of a request to communicate with another on-card Application;
- Checking for the validity of a request to access the GlobalPlatform Registry entry of another Application, including a Security Domain;
- Identifying the Application with Final Application privilege to be default selected when the card is in CARD_LOCKED or TERMINATED state.

The OPEN shall use the Privileges data element and the Implicit Selection parameter for each Application (where present) for controlling the following runtime behavioral requirements:

- Checking for the validity of a request to modify historical bytes; for dual interface (contact and contactless) cards, the modification applies to the historical bytes of the card interface(s) for

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0076

which the requesting on-card Application is registered as implicitly selectable; this feature should preferably be used on cards that support the Basic Logical Channel only.

6.7 The GlobalPlatform Trusted Framework

An APDU command is received by the Application's Security Domain (the Receiving Entity), which may be the Issuer Security Domain or a Supplementary Security Domain, and is unwrapped by the Security Domain before being passed on to the GlobalPlatform Trusted Framework. The objective is that the GlobalPlatform Trusted Framework forwards the unwrapped command to the Target Application indicated by the Receiving Entity.

The Target Application may use cryptographic services of the Security Domain available through the Secure Channel Session established by the Security Domain (e.g. sensitive data decryption). The Current Security Level viewed by the Target Application may differ from the Security Domain view depending on the Secure Channel Protocol and the authenticated off-card entity's Application Provider ID (e.g. ANY_AUTHENTICATED for the Target Application and AUTHENTICATED for the Security Domain).

Runtime Behavior

The GlobalPlatform Trusted Framework shall check that:

- The Receiving Entity has the Trusted Path privilege;
- The Receiving Entity is a Security Domain;
- The Target Application exists in the GlobalPlatform Registry and has enabled its 'Process Data' entry point;
- The Target Application has no multi-selection restrictions if it is already selected on another logical channel;
- The Target Application is associated with the currently selected Receiving Entity Security Domain.

If all checks are passed, the GlobalPlatform Trusted Framework passes the command to the Target Application through its GlobalPlatform Application interface.

The GlobalPlatform Trusted Framework and the Applications involved are shown in the following diagram. The process as used in personalization is described in more detail in section 7.3.3 - *Personalization Support*.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0077

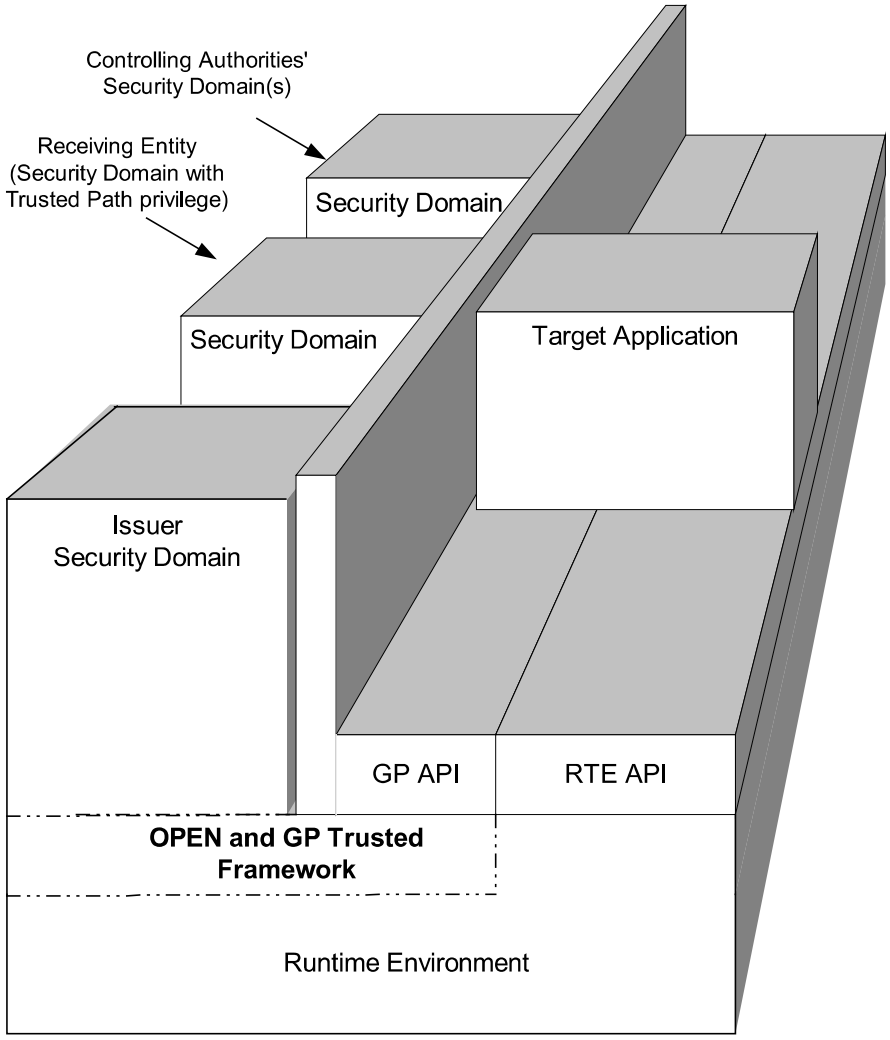


Figure 6-1: GlobalPlatform Trusted Framework Roles

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0078

7 Security Domains

7.1 General Description

Security Domains are privileged Applications. They hold cryptographic keys which can be used to support Secure Channel Protocol operations and/or to authorize card content management functions.

Each Application and each Executable Load File is associated with a Security Domain. An Application can use the cryptographic services of its associated Security Domain. It is possible to associate Applications owned by one authority with the Security Domain of another authority.

All cards have one mandatory Security Domain: the Issuer Security Domain. A card that supports multiple Security Domains can allow an Application Provider, through its own Security Domain, to manage its own Applications and provide cryptographic services using keys that are completely separate from, and not under the control of, the Card Issuer.

Key Separation

Security Domains are responsible for their own key management. This ensures that Applications and data from different Application Providers may coexist on the same card without violating the privacy and integrity of each Application Provider.

Application Services

The keys and associated cryptography for all Security Domains may be used for:

- Personalization Support: Secure communication support during personalization of an Application Provider's Applications;
- Runtime Messaging Support: secure communication support during runtime for an Application that does not contain its own secure messaging keys.

7.1.1 Issuer Security Domain

The Issuer Security Domain primarily operates as any Security Domain, but has some special characteristics that distinguish it from any other Security Domain:

- It is the first Application installed on a card. GlobalPlatform does not mandate that the Issuer Security Domain be loaded or installed in the same manner as Applications. The Issuer Security Domain, while viewed by the GlobalPlatform Registry as an Application, has implementation specific behavior relating to how it becomes an active entity on the card;
- It does not have a Security Domain Life Cycle State because it inherits the card Life Cycle State;
- It takes on the Card Reset privilege if the Application with that privilege is removed;
- It becomes the implicitly selected Application if the Application implicitly selectable on the same logical channel of the same card I/O interface is removed;
- It becomes the implicitly selected Application for a card interface on a logical channel if the Application that is implicitly selectable on that logical channel for that card interface is removed;
- It may be selected by use of the SELECT command with no command data field;
- It takes on the Final Application privilege if the Application with that privilege is removed.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0079

7.2 Security Domain Association

Applications (including Security Domains) may use the services of their associated Security Domain to provide Secure Channel Sessions and other cryptographic services. An Application need not have any prior knowledge of its Security Domain AID: the GlobalPlatform Registry contains this information and the OPEN supplies the Application with a reference to its associated Security Domain. The Application should not store this reference for future use because its associated Security Domain may change as a result of extradition.

Extradition is the means by which an Application is associated with a different Security Domain.

An Executable Load File is initially associated with the Security Domain which loads it, but it may immediately (implicit extradition during the load process) or subsequently (explicit extradition) be extradited to a different Security Domain.

The Issuer Security Domain is effectively associated with itself, its establishment on the card is not defined by GlobalPlatform, and it is not subject to extradition.

Through extradition, a Security Domain may be associated with itself. This means that if it calls on the services of its associated Security Domain, it will be using its own services.

As a result, there is one or more hierarchies of association on a card. The root of each hierarchy is a Security Domain that is associated with itself. The following diagram shows two hierarchies: one starting from the Issuer Security Domain, the other from a Security Domain which has been extradited to itself; arrows indicate 'is associated with'.

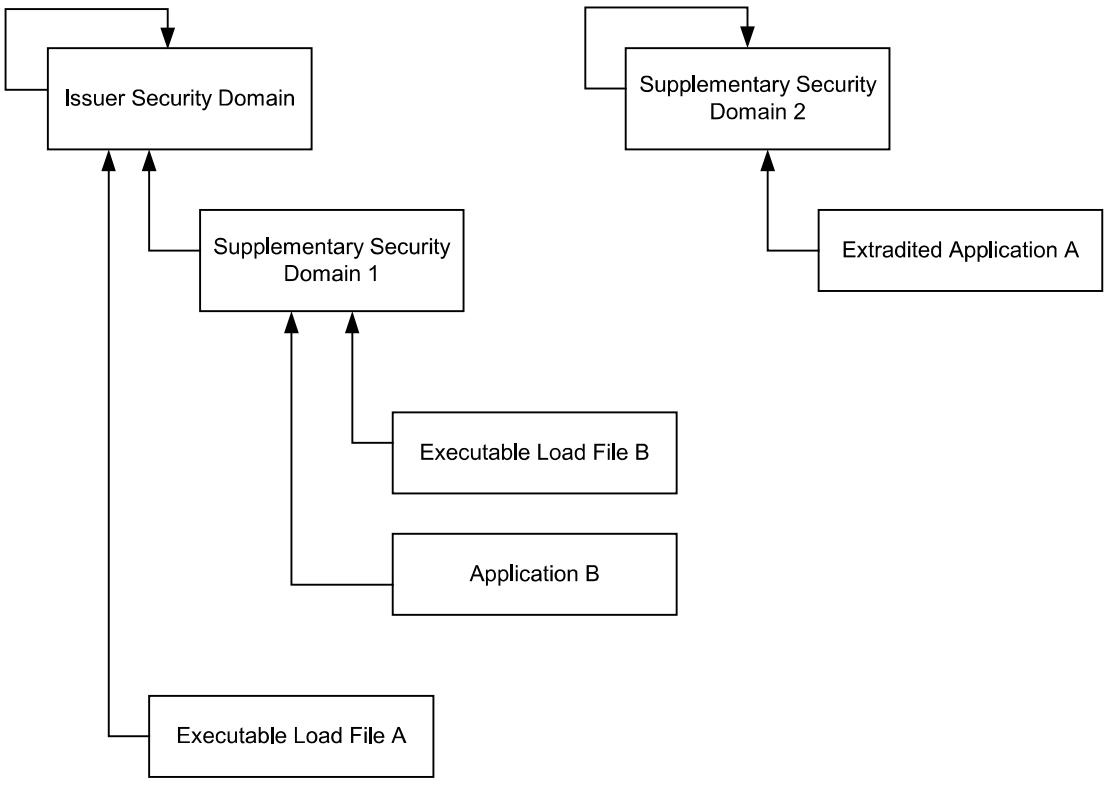


Figure 7-1: Example of Security Domain Hierarchies

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0080

A Security Domain associated with another Application is said to be directly associated with it. Another Security Domain higher up the hierarchy is said to be indirectly associated with it.

A sub-hierarchy of a Security Domain includes the Security Domain itself and all of the Security Domain's Applications and Executable Load Files below it in the same hierarchy.

7.3 Security Domain Services

Appendix A.1 - *GlobalPlatform on a Java Card* provides the Java Card™ specification of the following interfaces.

Appendix A.2 - *GlobalPlatform on MULTOS*™ provides the MULTOS™ specification of the following interfaces.

Appendix D - *Secure Channel Protocol '01' (Deprecated)*-, appendix E - *Secure Channel Protocol '02'* and appendix F - *Secure Channel Protocol '10'* provide more details on Secure Channel Protocols implementing the following interfaces.

7.3.1 Application Access to Security Domain Services

Applications have the ability to access the services of their associated Security Domain. By using these services, the Application may rely on cryptographic support from the Security Domain to ensure confidentiality and integrity during personalization and runtime. The Security Domain services defined in this Specification are generic and shall encompass the following possibilities.

- Initiating a Secure Channel Session upon successful verification of an off-card entity;
- Unwrapping a command received within a Secure Channel Session by verifying its integrity and/or decrypting the original data in the case of confidentiality;
- Controlling the sequence of APDU commands;
- Decrypting a secret data block;
- Setting the security level: integrity and/or confidentiality, to apply to the next incoming command and/or next outgoing response;
- Closing a Secure Channel Session upon request and destroying any secret(s) relating to that Secure Channel Session.

Depending on the specific Secure Channel Protocol supported, the Security Domain services may also encompass the possibility of:

- Wrapping a response sent within a Secure Channel Session by adding integrity and/or encrypting the original data in the case of confidentiality;
- Encrypting a secret data block;
- Controlling the sequence of APDU responses.

A Security Domain may support the management of multiple Secure Channel Sessions concurrently (i.e. Applications selected on multiple logical channels each initiating a Secure Channel) or may limit itself to only managing one Secure Channel Session immaterial of the number of concurrently selected Applications that attempt to use its services. If a Security Domain does support the management of multiple Secure Channel Sessions concurrently, it shall be able to differentiate between the multiple Secure Channel Sessions and their respective logical channels. If a Security Domain does not support the management of multiple Secure Channel Sessions concurrently, when a request is made to open a Secure Channel Session on a logical channel different from the current Secure Channel Session, the Security Domain rejects this request to initiate a new Secure Channel Session.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0081

If a request is made by an Application to use the services of its associated Security Domain on a logical channel different from the one on which its Secure Channel Session was opened, the Security Domain shall reject this request.

7.3.2 Security Domain Access to Applications

The Security Domain has the facility to receive a STORE DATA command destined to one of its associated Applications. The Security Domain unwraps this command according to the Current Security Level of the current Secure Channel Session and prior to the command being forwarded to the Application. This pre-processing leaves as is the data structures of the command message as well as the eventual encryption of the data value fields of these data structures.

The command is forwarded to the Application by the GlobalPlatform Trusted Framework which handles inter-application communication between Security Domains and Applications, as described in section 6.7.

7.3.3 Personalization Support

After an Application is installed, the Application may need to obtain its personalization data, including its own keys and Cardholder-specific data. The Application can utilize the secure communication and key decryption services of its associated Security Domain to manage the secure loading of this personalization data. This can be achieved in two ways: one being to utilize the runtime messaging support described in section 7.3.4 - *Runtime Messaging Support*, the other being to utilize the Security Domain's ability to access the Application as described in section 7.3.2.

This section addresses the second method.

Using this second method on a card that only supports the Basic Logical Channel allows the Application to be personalized without the Application being the selected Application. Rather the Security Domain is the selected Application and the Security Domain receives commands on behalf of the Application. The Security Domain would pre-process the personalization (STORE DATA) command prior to forwarding the command to the Application via the GlobalPlatform Trusted Framework.

Using this second method on a card that supports multiple logical channels differs slightly only in that the Application could have a multi-selection restriction in which case personalization would fail. If an Application does not support this second method, the Security Domain shall reject any STORE DATA command destined to this Application.

Runtime Behavior

On receipt of an INSTALL [for personalization] command and subsequent STORE DATA commands, the Security Domain performing the personalization of the Application shall:

- Apply its own secure communication policy;
- Check that the off-card entity is authenticated as the Application Provider;
- Pre-process subsequent STORE DATA commands according to the Current Security Level of the Secure Channel Session and prior to the command being forwarded to the target Application.

On receipt of a request to forward commands to an Application, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restrictions for personalization (see Table 11-53);
- Apply the GlobalPlatform Trusted Framework runtime requirements defined in section 6.7.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0082

Personalization Flow

The following diagram is an example of an Application receiving data from its associated Security Domain during personalization.

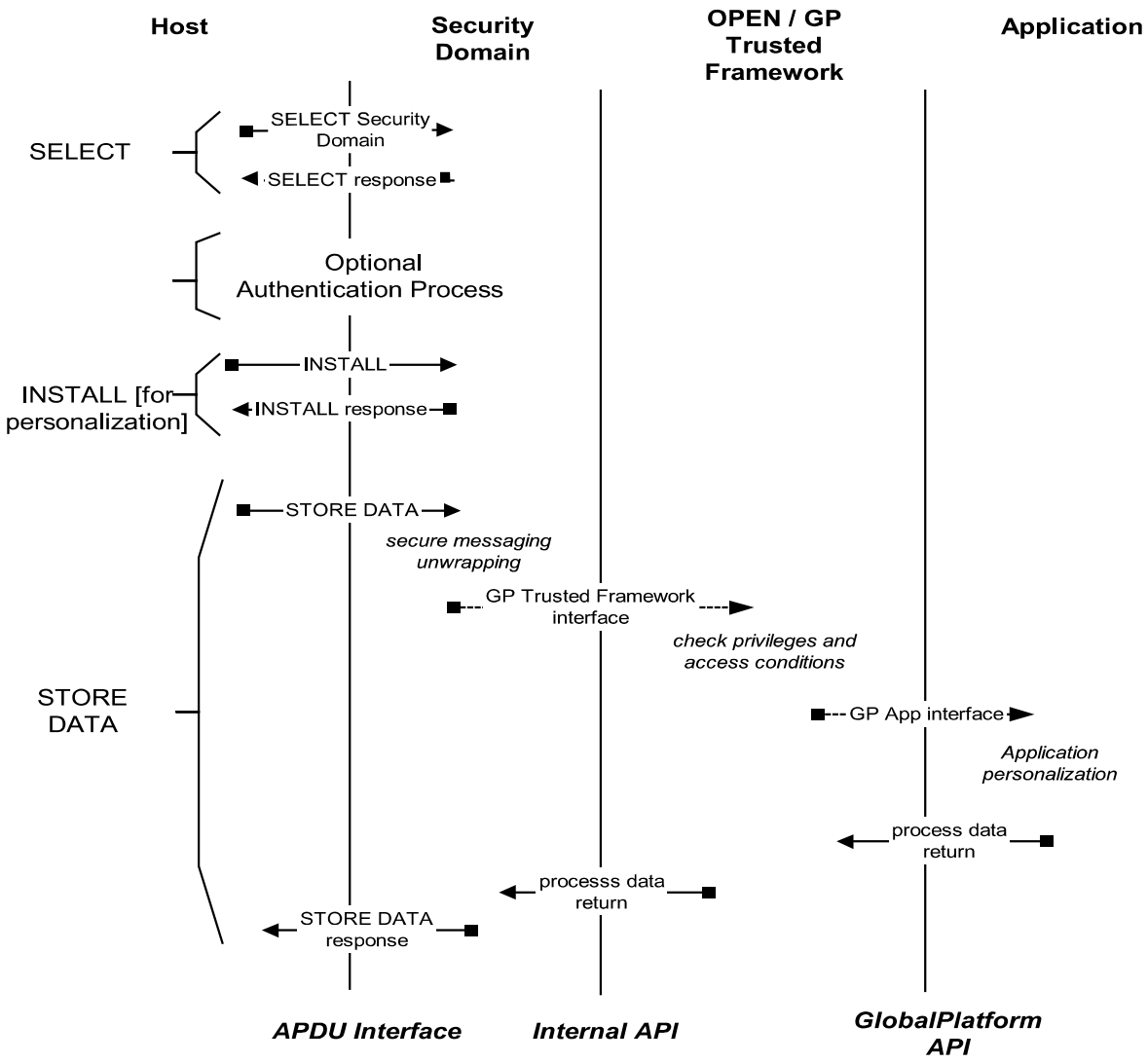


Figure 7-2: Application Personalization through Associated Security Domain

7.3.4 Runtime Messaging Support

Security Domains may provide runtime support for secure communication to their directly associated Applications. Instead of loading additional communication keys into an Application, the Application Provider may choose to use the associated Security Domain services for all Application communication throughout the life of the Application.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0083

Runtime Messaging Flow

The following diagram is an example of an Application using the services of its associated Security Domain:

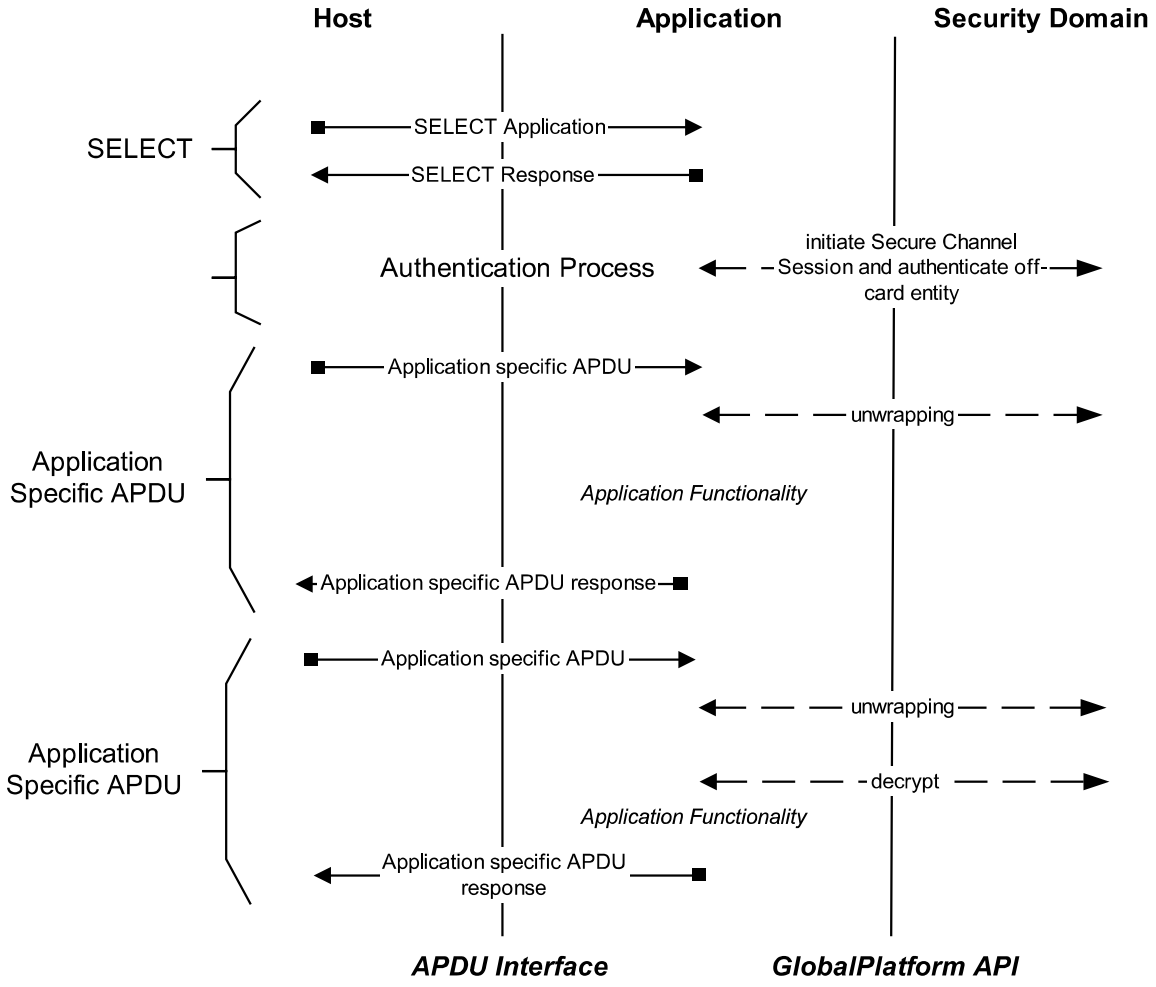


Figure 7-3: Runtime Messaging Flow

7.4 Security Domain Data

7.4.1 Issuer Security Domain

The Issuer Security Domain shall be able to handle the following data:

- Issuer Identification Number (IIN);
- Card Image Number (CIN);
- Card Recognition Data;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0084

- Other Card Issuer's proprietary data.

These data shall be available from the card using the GET DATA command.

7.4.1.1 Issuer Identification Number

The Issuer Identification Number (IIN) may be used by an off-card entity to associate the card with a specific Card Management System. The IIN typically contains the ISO 7812 defined identification of the Issuer and is carried by the ISO/IEC 7816-6 tag '42'. The IIN data element is of variable length.

7.4.1.2 Card Image Number

The Card Image Number (CIN) may be used by a Card Management System to uniquely identify a card within its card base. It is a unique value, carried by the ISO/IEC 7816 defined tag '45' (Card Issuer's Data), which is assigned by the Card Issuer (identified itself by the IIN). The CIN data element is of variable length.

7.4.1.3 Card Recognition Data

Card Management Systems need information about a card before they can start to interact with it. This includes the kind of card it is and what Secure Channel Protocol it supports.

Card Recognition Data is the mechanism for providing information about a card, and thus avoiding the vagaries of trial-and-error. See appendix H for details.

Card Recognition Data shall be present and contained in a data template (tag '73'). This template shall in turn be contained in the “Card Data” data object (tag '66'), as defined in ISO/IEC 7816-6. Card Data can be retrieved using the GET DATA command. (For contact cards according to ISO/IEC 7816-4, Card Data may also be accessed through the ATR, if a suitable “command to perform” is included in the ATR historical bytes.)

Note that the information provided in Card Recognition Data should be enough to enable initial communication with the card without resorting to trial and error. Information not essential for this purpose should be supplied during subsequent interaction with the card.

There is no specific requirement for Card Recognition Data to be updated dynamically by the card, but additional dynamic data objects are not precluded.

7.4.2 Supplementary Security Domains

Security Domains other than the Issuer Security Domain may handle their own identification data:

- A Security Domain Provider Identification Number (SIN);
- A Security Domain Image Number;
- Security Domain Management Data;
- Other Application Provider proprietary data.

When present, these data shall be available from the Security Domain using the GET DATA command.

7.4.2.1 Security Domain Provider Identification Number

The Security Domain Provider Identification Number (SIN) may be used by an off-card entity to associate the Security Domain with a specific Card Management System. It is an IIN, typically contains the ISO

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0085

7812 defined identification of the Security Domain provider, and is carried by the ISO/IEC 7816-6 tag '42'. The SIN data element is of variable length.

7.4.2.2 A Security Domain Image Number

The Security Domain Image Number may be used by an Application Management System to uniquely identify an instance of a Security Domain on a card. If used it is a unique value, carried by the ISO/IEC 7816 defined tag '45'.

7.4.2.3 Security Domain Management Data

Application Management Systems need information about a Security Domain before they can start to interact with it. This includes the kind of Security Domain it is and what Secure Channel Protocol it supports.

Security Domain Management Data is the mechanism for providing information about a Security Domain, and thus avoiding the vagaries of trial-and-error. Security Domain Management Data (tag '73') shall be returned in the response to the SELECT command when present. Security Domain Management Data shall also be returned in response to a GET DATA command with tag '66'.

Note that the information provided in Security Domain Management Data should be enough to enable initial communication with the card without resorting to trial and error.

There is no specific requirement for Security Domain Management Data to be updated dynamically by the card, but additional dynamic data objects are not precluded.

For further details refer to appendix H.

7.5 Security Domain Keys

7.5.1 Key Information

See the appropriate appendix D, E, or F for details of the keys used with each Secure Channel Protocol. See appendix C.1 for details of token, receipt and DAP keys.

Keys have the following attributes:

- A Key Identifier, which identifies each key within an on-card entity. A key may consist of one or more key components, e.g. a symmetric key has only one key component while an asymmetric key has several components. All key components share the same Key Identifier. Different Key Identifiers within one on-card entity shall be used to differentiate keys, their usage, and their functionality. There is no restriction and no pre-defined order in assigning Key Identifiers to keys, including non-sequential Key Identifiers within the same entity;
- An associated Key Version Number: different key versions within an on-card entity may be used to differentiate several instances or versions of the same key. There is no restriction and no pre-defined order in assigning Key Version Numbers to keys;
- An associated cryptographic algorithm: a specific key is associated with one and only one cryptographic algorithm;
- A length, for cryptographic algorithms supporting several key (or key component) lengths;
- Access conditions, to control and segment access to keys.

These key attributes together indicate unambiguously to the on-card entity:

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0086

- The identity;
- The intended usage;
- The functionality of cryptographic keys.

The combination of a Key Identifier and a Key Version Number identifies unambiguously a key within an on-card entity. The key type identifies the cryptographic algorithm and key component. Identifying unambiguously a key and an algorithm within an entity prevent the misuse of cryptographic functionality.

An off-card entity may obtain information on Security Domain key(s) with a GET DATA command for Key Information Template (tag ‘E0’).

A Security Domain manages keys as follows:

- A Key Identifier and Key Version Number uniquely reference each key within the on-card entity. In other words, each combination Key Identifier / Key Version Number identifies a unique key slot within that entity.
- Adding a key equates to allocating a new key slot with a new key value, a new Key Identifier, or a new Key Version Number.
- Replacing a key involves updating the key slot with a new key value and the associated Key Version Number. The Key Identifier remains the same. The previous key shall no longer be available.

The off-card key management system shall be aware of the scheme used to identify keys held by the on-card entity. Key Identifiers and Key Version Numbers may have arbitrary values for the card (e.g. not being sequential, not starting with '01') and these values may vary from one key management scheme to the next. Off-card key management schemes are outside the scope of this specification.

Any velocity checking related to a particular keys usage e.g. key try counters and limits are dependent on the Security Domain provider's security policy.

The Security Domain shall store all the Key Information supplied in the PUT KEY command in association with each key.

7.5.2 Key Access Conditions

The Access Conditions assigned to a Security Domain key are either:

- Owner only: the Security Domain itself;
- Authorized users other than the owner: e.g. the Security Domain’s associated Applications;
- Any authorized users, including the owner: e.g. the Security Domain and its associated Applications.

This version of the Specification defines the following Access Conditions for Security Domain keys, coded on one byte as follows:

- ‘00’: any authorized user, including the owner; this is the Access Condition by default for Secure Channel Protocol Keys, when not explicitly provided in the PUT KEY command;
- ‘01’: the owner only; this is the Access Condition by default for Token and DAP Keys, when not explicitly provided in the PUT KEY command;
- ‘02’: authorized users other than the owner;
- ‘03’ to ‘7F’: Reserved for Future Use by GlobalPlatform;
- ‘80’ to ‘FE’: Reserved for proprietary use;

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0087

- 'FF': not available.

The access control rules applicable to any Security Domain key are enforced as follows:

- In order to use any Security Domain's cryptographic service, the Application requests to the OPEN the reference of a Secure Channel interface; the OPEN identifies the Security Domain associated with the Application and provides the corresponding Secure Channel interface reference to the Application (GlobalPlatform Registry acting as an access control list);
- The Application requests cryptographic services to a Security Domain, via its Secure Channel interface; since the OPEN ensures access to associated Applications only, the Security Domain controls are simplified to enforce the Access Conditions applicable to each of its keys (e.g. rejecting requests for accessing a key with an Access Condition set to '01').

7.6 Data and Key Management

These services relate to the storing of cryptographic keys and data on the card.

Runtime Behavior

On receipt of a data/key management request, the corresponding Security Domain shall manage the data/key according to its own access control rules.

The card Life Cycle State shall not be CARD_LOCKED or TERMINATED.

On receipt of a DELETE [key], PUT KEY or STORE DATA command, the Security Domain performing the data or key management shall apply its own secure communication policy. The Security Domain provider may apply its own key management policy regarding deletion of keys.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0088

8 Global Platform Services

8.1 Global Services Applications

One or more Global Services Applications may be present on the card to provide services to other Applications on the card. Global Services Applications are distinguished from other Applications through a specific privilege: Global Service.

8.1.1 Registering Global Services

During the installation of an Application (see section 9.3.6 -*Card Content Installation*) or during the registry update for an already installed Application (see section 9.4 - *Content Extradition and Registry Update*), an Application may be assigned the Global Service privilege and optionally Global Service Parameters comprising one (or more) service name(s). When present, each service name identifies a service family and optionally a specific service identifier within that service family, identifying which service(s) the Global Services Application offers to other Applications. When present, the Global Service Parameters shall be recorded in the GlobalPlatform Registry entry for the Application. Uniqueness on the card of this (these) service name(s) is not required in order to allow more than one Global Services Application to offer similar services.

To offer a unique service onto a card, a Global Services Application may register a Global Service with a service name that is unique on that card. A Global Services Application may register one or more Global Service(s) with unique service name(s). OPEN is responsible for ensuring the uniqueness of each service name registered by Global Services Applications.

Runtime Behavior

The following runtime behavior requirements apply to the OPEN during the registration process of a Global Service with a unique service name. On receipt of unique service registration request, the OPEN shall:

- Check that the requesting on-card entity has the Global Service privilege;
- If one (or more) service name(s) are recorded for that on-card entity, check that the requested service name matches exactly with (one of) the service name(s) recorded for that on-card entity, or belongs to the same service family if the recorded service name(s) only identifies(y) service family(ies);
- Check that the requested service name is not registered within the GlobalPlatform Registry for another on-card entity;
- Register accordingly as unique the requested service name.

The following runtime behavior requirements apply to the OPEN during the deregistration process of a Global Service with a unique service name. On receipt of service deregistration request, the OPEN shall:

- Check that the requesting on-card entity has the Global Service privilege;
- Check that the requested service name is registered in the GlobalPlatform Registry entry of the requesting on-card entity;
- Deregister accordingly the requested service name as being unique.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0089

8.1.2 Application Access to Global Services

GlobalPlatform API is the interface Applications use to access Global Services. An Application may access a uniquely registered Global Service or a specific Global Services Application.

Runtime Behavior

The following runtime behavior requirements apply to the OPEN during the access of a uniquely registered Global Service or a specific Global Services Application. On receipt of service access request, the OPEN shall:

- If the request indicates a specific service name without any associated AID, check that the requested service name matches exactly with (one of) the service name(s) uniquely registered, or belongs to the same service family uniquely registered;
- If the request indicates a specific AID, check that the on-card entity identified in the request has the Global Service privilege, and that the requested service name matches exactly with (one of) the service name(s) recorded for that on-card entity, or belongs to (one of) the same service family(ies) recorded for that on-card entity;
- Identify the corresponding Global Services Application;
- Obtain the GlobalPlatform Service interface of the corresponding Global Services Application and forward it to the requesting on-card entity.

The requesting on-card entity can then directly invoke the GlobalPlatform Service interface of the corresponding Global Services Application and authenticate itself in order to obtain the requested service.

8.1.3 Global Service Parameters

Global Service Parameters may be defined for an Application and list one or more service names. Each service name is coded on two bytes. The first byte identifies the service family, the second the service id within that family. The following values are assigned to the service family identifier:

- '00' to '7F' – Reserved for proprietary use and not registered by GlobalPlatform,
- '80' to '9F' – Reserved for use by GlobalPlatform
  - '80' – Not available,
  - '81' – GlobalPlatform Secure Channel,
  - '82' – GlobalPlatform CVM;
- 'A0' to 'FE' – Reserved for use by individual schemes registered by GlobalPlatform;
  - 'A0' – USSM;
- 'FF' – Not available;

The values assigned to the service id within a service family are specific to each service family.

- A service id value of '00' is typically reserved to indicate ‘any service id within that family’; or may be used as a default value in the case where the service family does not require a service identifier;
- For the GlobalPlatform Secure Channel family, the Secure Channel Protocol identifiers (see 10.7 - *Secure Channel Protocol Identifier*) are the assigned service id values for that family;
- For the GlobalPlatform CVM family, the CVM identifier values (see section 8.2.2.1 - *Registering CVM*) are the assigned service id values for that family.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0090

8.2 CVM Application

The CVM Application, if present on a card, provides a mechanism for a Cardholder Verification Method (CVM), including velocity checking, that may be used by all Applications on the card. In this version of the Specification there is one CVM standardized by GlobalPlatform: the global Personal Identification Number (global PIN).

The CVM verification services may be accessed by any Application. CVM management services shall only be accessible to privileged on-card Applications. The CVM application may also offer CVM management services to suitably authenticated off-card entities through an APDU interface that is beyond the scope of this specification.

A CVM Application may support multiple CVMs, and there may be more than one CVM Application present on a card. Each CVM shall have a unique CVM identifier, which shall be unique across the whole card. The standardized CVM (global PIN), if present on a card, shall be given the CVM identifier of '11'.

For each CVM supported, the CVM Application shall:

- Hold securely CVM management data: CVM value, CVM State, CVM Retry Limit, and CVM Retry Counter;
- Perform CVM-specific risk management, such as internal velocity checks on the CVM to prevent card and Application access violations;
- Implement one or more CVM interfaces;
- Request the OPEN to register the CVM identifier if that CVM is unique;
- Provide the CVM services to Applications;
- Manage the CVM state;
- Manage the CVM Retry Limit and CVM Retry Counter.

Depending on the Issuer policy, a value for the Retry Limit may be set by default.

8.2.1 Application Access to CVM Services

The following CVM services shall be provided by a CVM Application to other on-card Applications:

- Retrieving the CVM state (e.g. to determine if the CVM value has been submitted, verified or blocked);
- Retrieving the number of remaining times the CVM value can be incorrectly presented prior to the CVM being blocked;
- Setting a new value for the CVM value. This depends on the requesting Application having the CVM Management privilege;
- Verifying the content of an incoming CVM value by comparing the incoming CVM value to the stored CVM value;
- Setting the maximum number of times the CVM value can be incorrectly presented prior to the CVM being blocked. This depends on the requesting Application having the CVM Management privilege.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0091

8.2.2 CVM Management

8.2.2.1 Registering CVM

In order to offer unique CVM services that are accessible by other Applications, a CVM Application shall register with the OPEN the CVM identifier(s) for which it offers services. The OPEN shall ensure that the registered CVM identifiers are unique on the whole card. Reuse is only possible if the CVM identifier is deregistered or the corresponding CVM Application is deleted.

The following values are assigned to CVM identifiers:

- '00' - Not available;
- '01' to '7F' - Reserved for use by GlobalPlatform;
  - '01' to '10' - PIN as defined in ETSI TS 102 221 specification;
  - '11' - Global PIN;
  - '12' to '1F' - PIN as defined in ETSI TS 102 221 specification;
- '80' to 'EF' - Reserved for use by individual schemes registered by GlobalPlatform;
  - '81' to '9F' - PIN as defined in ETSI TS 102 221 specification;
- 'F0' to 'FF' - Reserved for proprietary use and not registered by GlobalPlatform.

8.2.2.2 CVM States

The CVM state may be used by a CVM Application to assist in managing CVM services. The non-atomic states of the CVM may be seen within a Card Session. The CVM state, the Retry Limit, and the Retry Counter are closely related. All CVM state transitions are immediately visible to the Application that caused the transition as well as to any Applications that may be selected on other logical channels.

The CVM states are:

- ACTIVE
- INVALID_SUBMISSION
- VALIDATED
- BLOCKED

8.2.2.2.1 CVM State ACTIVE

The CVM state shall first become ACTIVE when both the CVM value and the Retry Limit are set. The CVM state may also transition back to ACTIVE from any other CVM state if a privileged Application unblocks the CVM or changes the CVM value. Changing the CVM value shall also reset the Retry Counter. At the end of a Card Session the CVM state shall transition back to ACTIVE, except if the CVM state transitioned to the CVM state BLOCKED during the Card Session. The end of the Card Session shall not reset the Retry Counter.

8.2.2.2.2 CVM State INVALID_SUBMISSION

During the CVM verification, the CVM state shall transition to INVALID_SUBMISSION if the CVM verification fails. The Retry Counter shall be updated.

The CVM state shall remain INVALID_SUBMISSION until:

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0092

- The Card Session ends;
- A valid CVM verification is performed;
- An Application resets the CVM state;
- A privileged Application either blocks the CVM or changes the CVM value or CVM Retry Limit;
- Subsequent CVM verification(s) fail causing the CVM state to transition to BLOCKED.

8.2.2.2.3 CVM State VALIDATED

During CVM verification, the CVM state shall transition to VALIDATED and the Retry Counter shall be reset if the CVM verification is successful.

The CVM state shall remain VALIDATED until:

- The Card Session ends;
- An invalid CVM verification is performed;
- An Application resets the CVM state;
- A privileged Application either blocks the CVM, or changes the CVM value or CVM Retry Limit.

8.2.2.2.4 CVM State BLOCKED

During CVM verification, if the CVM verification fails and the Retry Limit has been reached, the CVM state shall transition to BLOCKED. The CVM state may also transition to BLOCKED if a privileged Application initiates this transition. The BLOCKED state shall not transition when the Card Session ends. The CVM state may only transition from the BLOCKED state back to the ACTIVE state on instruction from a privileged Application, which either resets (unblocks) the CVM state or changes the CVM value or CVM Retry Limit. The CVM verification shall always fail in the BLOCKED state.

8.2.2.3 CVM Format

The 3 following formats are defined for the CVM value:

- Format BCD includes only numerical digits, coded on a nibble (4 bits), left justified, and eventually padded on the right with an 'F' nibble if necessary (i.e. the number of digits is odd);
- Format ASCII includes all displayable characters (alphabetic, numerical, and special) and space (i.e. format ASCII ranges from ‘20’ to ‘7E’), coded on one byte and left justified.
- Format HEX is equivalent to a transparent mode (“as is”) and includes all binary values coded on one byte.

The following rules apply for the CVM format conversion:

- No conversion from and to HEX format is valid;
- Conversion from BCD format to ASCII format is valid: the numeric nibbles are expanded to the corresponding characters coded on one byte and the padding nibble 'F' is deleted (if present);
- Conversion from ASCII format to BCD format is valid for numeric characters only: the numeric characters coded on one byte are converted to numeric nibbles, padded together in bytes, and a padding nibble 'F' is added on the right if necessary.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0093

The internal format for storing the CVM value by a CVM Application is implementation dependent and shall be transparent to any other on-card Application that uses CVM services. It shall not preclude any format used by Applications requesting CVM services.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0094

9 Card and Application Management

9.1 Card Content Management

9.1.1 Overview

Card Content management on a GlobalPlatform card is the capability for the loading, installation, extradition, registry update and removal of Card Content. GlobalPlatform is designed for providing maximum flexibility to the Card Issuer and its business partners regarding Card Content management. The design of the GlobalPlatform takes into account the possibility that the Card Issuer may not necessarily want to manage all Card Content changes, especially when the Card Content does not belong to the Card Issuer.

Thus the Card Issuer may delegate Card Content management to an Application Provider with or without authorization:

- It may authorize all Card Content management operations performed by an Application Provider;
- It may authorize an Application Provider to have full control of its Card Content;
- It may authorize an Application Provider to isolate its own Security Domain(s) and Application(s) from other Application Providers, and potentially from the Card Issuer itself.

Card Content changes are permitted according to the privileges that have been assigned to the various Security Domains on the card.

The following sections describe the OPEN and Security Domain requirements to support the operation and authorization of Card Content management.

9.1.2 OPEN Requirements

The OPEN:

- Performs the physical loading and installation;
- May prohibit more than one Card Content management operation occurring concurrently;
- Prohibits Card Content management in the card Life Cycle States CARD_LOCKED or TERMINATED.

9.1.3 Security Domain Requirements

The Security Domain through which Card Content management is performed applies its own secure communication policy, which should be checked for consistency with any Card Issuer policies before the Security Domain is installed.

Card Content management involves a Security Domain performing loading, installation, extradition, update to GlobalPlatform Registry and content removal operations.

9.1.3.1 Security Domain with Token Verification Privilege

The privilege allows a Security Domain Provider, to authorize Card Content management operations. Within a sub-hierarchy of Security Domains starting from the Security Domain with the Authorized

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0095

Management Privilege, the Security Domain having the Token Verification privilege controls such authorization. A Security Domain with Token Verification privilege requires the knowledge of keys and algorithms used for Tokens.

Note: Typically, the Token Verification privilege is assigned to a Security Domain with the Authorized Management privilege. The Token Verification privilege does not provide Card Content Management capability.

In this version of the specification, it is assumed that within a sub-hierarchy, starting from a Security Domain with the Authorized Management privilege, no more than one Security Domain may have the Token Verification privilege.

9.1.3.2 Security Domain with Authorized Management Privilege

Having a Security Domain with this privilege allows a Security Domain provider to perform Card Content management without authorization (i.e. a token) in the case where the off-card entity is authenticated as the owner (Security Domain Provider) of the Security Domain. In that case the Security Domain that has Token Verification privilege is not involved. However, a Token is still required if the off-card entity is authenticated but is not the Security Domain Provider (see section 10.4 - *Entity Authentication*). A Security Domain with the Authorized Management privilege may delegate the Card Content Management operation on its descendant load files and applications.

9.1.3.3 Security Domain with Delegated Management Privilege.

The Delegated Management privilege allows an Application Provider's Security Domain with this privilege to perform:

- Delegated loading;
- Delegated installation and make selectable;
- Delegated extradition;
- Delegated update to the GlobalPlatform Registry;
- Delegated deletion.

The privilege allows an Application Provider to manage Card Content with authorization. Within a sub-hierarchy of Security Domains starting from the Security Domain with the Authorized Management privilege, the descendant Security Domain having the Token Verification privilege controls such authorization. In this version of the specification, it is assumed that the Security Domain with the Delegated Management privilege performs card content operations only within the sub-hierarchy starting from a Security Domain with the Authorized Management privilege.

Delegated Management is not a mandated feature of a GlobalPlatform card and is only necessary for Card Issuers that choose to offer this flexibility. In order to achieve it, close co-operation is required between the OPEN and the Security Domains.

9.1.3.4 Security Domain with Global Delete Privilege

This privilege provides the capability to remove any Executable Load File or Application from the card even if the Executable Load File or Application does not belong to this Security Domain.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0096

9.1.3.5 Security Domain with Global Lock Privilege

This privilege provides the right to initiate the locking and unlocking of any Application on the card, independent of its Security Domain association and hierarchy. It also provides the capability to restrict the Card Content Management functionality of OPEN.

9.1.3.6 Security Domain with Receipt Generation Privilege

This privilege allows a Security Domain Provider, to provide a confirmation for a delegated card content management operation. Within a sub-hierarchy of Security Domains starting from the Security Domain with the Authorized Management privilege, the descendant Security Domain with Receipt Generation privilege shall generate the receipt. It requires the knowledge of keys and algorithms used for Receipt generation. It shall also keep track of a Confirmation Counter that is incremented when generating each Receipt. When reaching its maximum value, the Confirmation Counter shall not be reset to zero. Security Domains are not required to support counter values beyond 32767.

Note that this privilege does not provide Card Content management capability.

In this version of the specification, it is assumed that within a sub-hierarchy, starting from a Security Domain with the Authorized Management privilege, no more than one Security Domain may have the Receipt Generation privilege.

9.1.3.7 Ciphered Load File Data Block Privilege

This privilege allows a Security Domain Provider to require that the Load File Data Block being associated to it shall be ciphered.

9.2 Authorizing and Controlling Card Content

The following section details the authorization and control features that may be used during Card Content loading and installation. The responsibility of ensuring that these controls are present when required rests with the OPEN.

9.2.1 DAP Verification

An Application Provider may require that their Application code to be loaded on the card shall be checked for integrity and authenticity. The DAP Verification privilege of the Application Provider's Security Domain detailed in this Specification provides this service on behalf of an Application Provider.

A Controlling Authority may require that all Application code to be loaded onto the card shall be checked for integrity and authenticity. The Mandated DAP Verification privilege of the Controlling Authority's Security Domain detailed in this Specification provides this service on behalf of the Controlling Authority.

The key and algorithm to be used for DAP Verification or Mandated DAP Verification are implicitly known by the corresponding Security Domain.

Flow control and runtime behavior as described in section 9.3.5 - *Card Content Loading Process* applies; more detail on DAP Blocks is provided in appendix C.3.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0097

9.2.2 Load File Data Block Hash

The Load File Data Block Hash is an integrity check across the whole Load File Data Block to be transferred to the card and is present as a field in the INSTALL [for load] command; more detail is provided in appendix C.2. The Load File Data Block Hash is mandatory when a Token or DAP Block is present in a Load File, and is optional otherwise. If a Load File Data Block Hash is present in a Load File, then it shall be checked.

See appendix B.2.1 - *Secure Hash Algorithm (SHA-1)* for more details on the hash algorithm.

Flow control and runtime behavior as described in section 9.3.5 - *Card Content Loading Process* applies.

9.2.3 Tokens

Tokens relate specifically to Delegated Management, and to Authorized Management where the off-card entity is not the Security Domain Provider. They are not allowed in other cases. More detail is provided in appendix C.4. The entity owning the Security Domain with Token Verification Privilege provides a Token to the Security Domain Provider performing the content management function. During the processing of the content management function the token is verified on-card by the Security Domain with Token Verification Privilege.

9.3 Card Content Loading, Installation and Make Selectable

9.3.1 Overview

The GlobalPlatform Card Content loading process is designed to allow the addition of code to Mutable Persistent Memory in the card. Card Content loading may be prohibited if a load process is already in progress on another logical channel.

The GlobalPlatform Card Content installation process is designed to allow the Card Issuer to make previously loaded application code executable on the card.

Card Content installation is either performed simultaneously with the load process, immediately following the load process or at a later time.

The Load File Data Block contains the information required in order to create an Executable Load File. The internal organization of the Load File Data Block is beyond the scope of this Specification. The Java Card™ CAP file definition and MULTOS™ Application Load Unit are examples of an expected Load File Data Block. The Load File Data Block may also contain information on the Load File Data Block attributes such as its name, version number and size. The Card Content loading and installation process may include implementation specific linking and actual verification of the executable code. Additional authentication data may also be present in the Load File.

Upon the successful completion of the Card Content loading, an Executable Load File shall be present on the card and the OPEN shall create an entry in the GlobalPlatform Registry for the Executable Load File. The OPEN shall also create an entry in the GlobalPlatform Registry for each Executable Module present within an Executable Load File. However, Executable Modules are not yet ready for execution. Applications may then be installed. Installing an Application results in another entry in the GlobalPlatform Registry.

Figure 9-1 details the two possible phases of the Card Content loading and installation.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0098

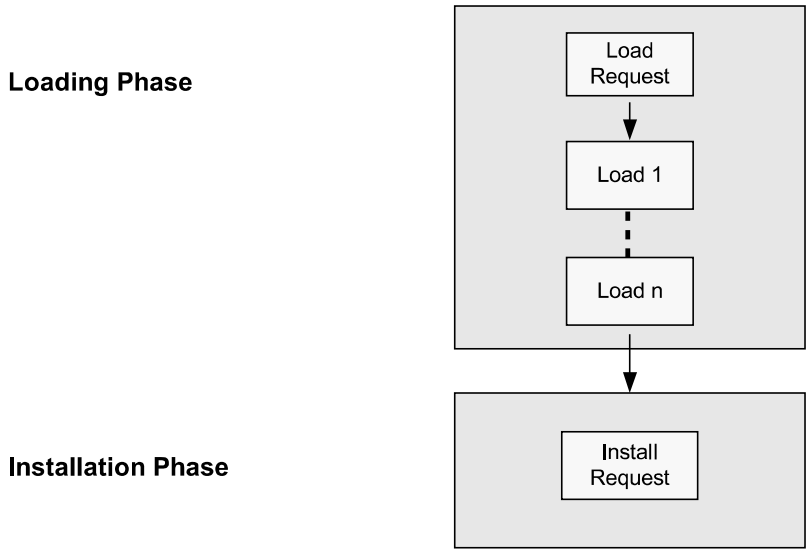


Figure 9-1: Loading and Installation Process

9.3.2 Card Content Loading

When requested to do so by the OPEN, the Security Domain with Token Verification privilege shall verify the transmission of the Load File from the off-card entity to the card, and when applicable, Security Domains with the relevant privilege shall verify the integrity of the Load File Data Block before the OPEN commits the new content to memory.

A Security Domain with Authorized Management or Delegated Management privilege may load an Executable Load File to any Security Domain. The Executable Load File is subject to acceptance by the receiving Security Domain where applicable.

The load process comprises an INSTALL [for load] command and one or more LOAD commands all of which are processed by the Security Domain. The Security Domain then passes the load request and Load File information to the OPEN for additional verification and processing.

The Load Token allows the OPEN, via the Security Domain with Token Verification privilege within the same sub-hierarchy as the Security Domain performing the load, to ensure that the Token authorized the load process and the loading of the content of the Load File Data Block.

The Load File Data Block Hash links the Token to the actual Load File Data Block.

The response to the last LOAD command identifies the end of the load process. Following the completion of the load process, an optional Load Receipt is returned to the Security Domain performing the Delegated Management operation and shall be transmitted by the Security Domain to the off-card entity.

The Application Provider may then forward the Load Receipt to the corresponding off-card entity as a proof that the loading process was successfully performed. The purpose of the optional Load Receipt is to assist the Application Provider in keeping its Card Management System synchronized with its on-card application base.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0099

9.3.3 Card Content Installation

A Security Domain with Authorized Management or Delegated Management privilege may install an Application in the Security Domain that the Executable Load File is associated with. If the Security Domain performing the installation is not the Security Domain the Executable Load File is associated with, then this is referred to as implicit extradition of the Application and is subject to the rules in section 9.4 - *Content Extradition and Registry Update*.

The installation process comprises an INSTALL [for install] command processed by the Security Domain. The Security Domain then passes the install request to the OPEN for additional verification and processing.

The Install Token allows the OPEN, via the Security Domain with Token Verification privilege within the same sub-hierarchy as the Security Domain performing the installation, to ensure that the Token authorized the installation process.

The response to the INSTALL [for install] command identifies the end of the installation process. Following the completion of the installation process, an optional Install Receipt is returned to the Security Domain performing the Delegated Management operation and shall be transmitted by the Security Domain to the off-card entity.

The Application Provider may then forward the Install Receipt to the corresponding off-card entity as a proof that the installation process was successfully performed. The purpose of the optional Install Receipt is to assist the Application Provider in keeping its Card Management System synchronized with its on-card application base.

9.3.4 Card Content Combined Loading, Installation and Make Selectable

When requested to do so by the OPEN, the Security Domain with Token Verification privilege shall verify the transmission of the Load File from the off-card entity to the card, and when applicable, Security Domains with the relevant privilege shall verify the integrity of the Load File Data Block before the OPEN commits the new content to memory.

A Security Domain with Delegated Management privilege may load an Executable Load File to any Security Domain, install an Application from the Executable Load File and make the Application selectable.

The combined load, install and make selectable process comprises a first INSTALL [for load, install and make selectable] command, one or more LOAD commands and a last INSTALL [for load, install and make selectable] command all of which are processed by the Security Domain. The Executable Load File is subject to acceptance by the receiving Security Domain where applicable.

The combined Load, Install and Make Selectable Token allows the OPEN, via the Security Domain with Token Verification privilege within the same sub-hierarchy as the Security Domain performing the combined Load, Install and Make Selectable, to ensure that the Token authorized the load process and the loading of the content of the Load File Data Block as well as the installation of an Application from the previously loaded Executable Load File.

The response to the last INSTALL [for load, install and make selectable] command identifies the end of the combined load and install process. Following the completion of the load and install process, an optional combined Load, Install and Make Selectable Receipt is returned to the Security Domain performing the Delegated Management operation and shall be transmitted by the Security Domain to the off-card entity.

The Application Provider may then forward the combined Load, Install and Make Selectable Receipt to the corresponding off-card entity as a proof that the loading process was successfully performed. The purpose of the optional combined Load, Install and Make Selectable Receipt is to assist the Application Provider in keeping its Card Management System synchronized with its on-card application base.

Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Petitioner Samsung Ex-1006, 0100