GLOBALPLATFORM

ADVANCING STANDARDS FOR SMART CARD GROWTH

Card Specification 2.1.1
Release Notes

June 2003

Table of Contents

1. Revisions for version 2.1.1

Section 1.5.3 of GlobalPlatform Card Specification version 2.1.1 describes at a high-level the differences with version 2.1 of the specification as follows:

"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.

1.5.3.1 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.

1.5.3.2 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.

1.5.3.3 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.

1.5.3.4 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."

2. Errata and Precisions of version 2.1

The following table lists all the Errata and Precisions of version 2.1 of GlobalPlatform Card Specification incorporated in version 2.1.1 of GlobalPlatform Card Specification. Errata and precisions are classified in a sequential order that reflects the Card Specification index. Regular font is used for referencing version 2.1.1 section numbers and, when different, *italics* are used for referencing *version 2.1 section numbers*.

Note: Version 2.1 Errata and Precision List 0.5 would have been published if it had not been directly incorporated into version 2.1.1: these errata and precisions are referenced (respectively) as E.5.x and P.5.x.

Errata / Precision number	Version 2.1.1 section number (*version 2.1 section*)	Description
P.5.1	section 5.1.1.4	Card Life Cycle State CARD_LOCKED
P.2.1	section 5.3.1.5	Application Life Cycle Specific State Transitions
E.2.1	section 5.3.2.4	Security Domain Life Cycle State LOCKED
P.3.1	sections 5.3.2.4, 7.5	Security Domain Life Cycle State LOCKED and DAP verification
P.1.3	section 6.4.1	Figure 6-3 Load and Installation Flow Diagram
P.3.4	sections 6.4.1, 9.5.2.3.1	Load File AID in the INSTALL [for load] command
P.3.2	section 6.4.2.1	Security Domain deletion
P.5.2	sections 6.4.2.1, 6.4.2.2	Application and Executable Load File deletion: handling interruption

Errata / Precision number	Version 2.1.1 section number (*version 2.1 section)*	Description
P.5.9	section 6.5, appendix C.4	Receipt Confirmation Counter management
P.3.3	sections 6.9.1.2, 6.9.1.3, 6.9.1.4	Resetting the CVM State
P.1.4	section 6.9.2, appendix A.2	CVM format and format conversion for GlobalPlatform API CVM.update() and CVM.verify() methods
P.5.3	section 7.3	Pre-processing of STORE DATA commands for Application personalization
P.5.10	section 7.7.4, appendix C.4.2	No Receipt for INSTALL [for make selectable] and INSTALL [for personalization]
E.5.3	section 9	GET DATA requirements in Table 9-1
P.5.11	section 9.1	RFU bits
E.5.1	section 9.1.7	Receipt format: Confirmation Counter length
E.2.2	sections 9.3.1, 9.3.3.1	Key Information using GET DATA command
P.4.1	section 9.4.2.2	Get Status Parameter P2
P.5.4	section 9.4.2.2	GET STATUS command: error on parameter P2
P.3.5	section 9.5.2.3.1, appendix C.2	Load File Data Block Hash in the INSTALL [for load] command
E.2.3	sections 9.1.5, 9.6.2, 9.8.2 (*9.7.2*), 9.11.2 (*9.10.2*)	Maximum size of APDU commands
P.3.6	section 9.8.1 (*9.7.1*)	Key replacement with the same key identification attributes
E.3.1	section 9.8.3.2 (*9.7.3.2*)	PUT KEY command status words coding
P.3.7	section 9.9.2.3 (*9.8.2.3*)	SELECT Command with no data
E.2.4	section 9.10.2.2 (*9.9.2.2*)	SET STATUS command parameter P2
P.2.2	section 9.10.2.2 (*9.9.2.2*)	SET STATUS command: Life Cycle State transitions
E.1.4	section 9.11.2 (*9.10.2*)	Le for STORE DATA command
P.2.8	appendix A.2	AID value for Java Card Export File for GlobalPlatform API
P.1.5	appendix A.2	Atomicity for GlobalPlatform API on Java Card and GlobalPlatform API CVM.verify() method
P.2.3	appendix A.2	GlobalPlatform API invocation from within install() method
E.1.2	appendix A.2	Naming of GlobalPlatform interface CVM for Java Card
E.3.2	appendix A.2	GlobalPlatform API: SecureChannel.processSecurity() method exception coding
P.2.5	appendix A.2	GlobalPlatform API: SecureChannel.decryptData() & SecureChannel.encryptData() method errors
P.1.6	appendix A.2	GlobalPlatform API: SecureChannel.encryptData() method exceptions
P.2.6	appendix A.2	GlobalPlatform API: SecureChannel.unwrap() method errors
P.5.5	appendix A.2	GlobalPlatform API: SecureChannel.unwrap() method returned length and unwrapped command Lc value
P.5.6	appendix A.2	GlobalPlatform API: SecureChannel.unwrap() method and R-MAC computation

Errata / Precision number	Version 2.1.1 section number (*version 2.1 section)*	Description
P.1.7	appendices A.2, D.1.6, E.1.5	GlobalPlatform API: SecureChannel.getSecurityLevel() method response and Secure Channel Protocols Security Level
P.2.4	appendix A.2	GlobalPlatform API: GPSystem.setATRHistBytes() method errors
P.3.8	appendix A.2	GlobalPlatform API: CVM.update() and CVM.setTryLimit methods
P.5.7	appendix C.3.2	Token for INSTALL [for make selectable]
E.4.1	appendices C.4, C.4.1, C.4.2, C.4.3, C.4.4	Receipt generation algorithm
E.5.2	appendices C.4.1, C.4.2, C.4.3, C.4.4	Receipt format: Card Unique Data length
E.1.1	appendices D.1.1, E.1.1	Coding of Secure Channel Protocols Implementation Option “i”
E.2.5	appendices D.3.4, E.4.6	APDU Data Field Encryption and Decryption
E.2.6	appendices D.4.2.2, E.5.2.2	Le for EXTERNAL AUTHENTICATE command
P.5.8	appendix E.1.2	Secure Channel Protocol ‘02’: Sequence Counter management
E.5.4	appendix E.1.2.2	R-MAC session initiation
P.1.8	appendix E.1.2.2	Sequence Counter and session key generation in Secure Channel Protocol ‘02’
E.1.3	appendices E.4.2.1, E.4.2.2	Secure Channel Protocol ‘02’: Authentication Cryptograms computation
P.3.9	appendix E.4.5	Length of Response Data in R-MAC and R-MAC generation figure
E.2.7	appendix E.4.7	Secure Channel Protocol ‘02’: Sensitive Data Encryption and Decryption
P.1.9	appendices E.5.3.2, E.5.3.4	Coding of P2 for BEGIN R-MAC SESSION command
P.1.10	appendices E.5.4.2, E.5.4.3, E.5.4.4	Coding of P1 and P2 for END R-MAC SESSION command
P.1.1	appendix F.1	GlobalPlatform Object Identifier (OID) Value
P.1.2	appendix F.1	GlobalPlatform Registration Identifier (RID) Value
P.2.7	appendix F.1	Card Recognition Data Object Identifier value
P.3.10	appendix F.1	Default AID value for Issuer Security Domain
E.5.5	appendices F.1, F.2	ISO specification reference for OID coding

3. Logical channels

Support of logical channels is a new optional feature of version 2.1.1 of the GlobalPlatform Card Specification. The following table lists all the impacts of this new feature. Impacts are classified in a sequential order that reflects the Card Specification index.

Version 2.1.1 section number	Description
Section 1.3	Terminology and definitions
Section 3.2.1	OPEN functionality
Section 4.2.4.1	Runtime Environment Security Requirements
Section 6.1.1	OPEN Command Dispatch
Section 6.3	Command Dispatch and Application Selection
Section 6.3.1	Basic Logical Channel concept
Sections 6.3.1.1, 6.3.1.1.1, 6.3.1.1.2	Implicit and Explicit Application Selection on Basic Logical Channel
Section 6.3.1.2	Logical Channel Management on Basic Logical Channel
Section 6.3.1.3	Application Command Dispatch on Basic Logical Channel
Section 6.3.2	Supplementary Logical Channel concept
Sections 6.3.2.1, 6.3.2.1.1, 6.3.2.1.2	Implicit and Explicit Application Selection on Supplementary Logical Channel
Section 6.3.2.2	Logical Channel Management on Supplementary Logical Channel
Section 6.3.2.3	Application Command Dispatch on Supplementary Logical Channel
Section 6.4	Simultaneous Card Content management
Section 6.4.1	Card Content Loading
Section 6.4.1.2	Card Content Installation
Section 6.4.2	Application Removal
Section 6.6.2.4	Default Selected Application Privilege
Section 6.7.1	Application Locking
Section 6.7.2	Card Locking
Section 6.7.3	Card Termination
Section 6.9.1	CVM States
Section 7.2.1, Appendix A.2	Application Access to Security Domain Services and GlobalPlatform interface SecureChannel for Java Card
Section 7.3	Personalization Support
Sections 8, 8.1	Secure Communication and Secure Channel Session
Section 8.2.3	Secure Channel Termination
Section 9	New command: MANAGE CHANNEL, new entry in Table 9-2
Section 9.1.4	New values for class byte
Section 9.7	New section for MANAGE CHANNEL command
Appendix A.2	Logical Channels with Java Card 2.2 specifications
Appendix D.3.3	Secure Channel Protocol ‘01’: C-MAC generation and verification
Appendix E.4.4	Secure Channel Protocol ‘02’: C-MAC generation and verification
Appendix E.4.5	Secure Channel Protocol ‘02’: R-MAC generation and verification

4. Content Removal extension

The simultaneous deletion of an Executable Load File and all its related Applications is a new optional feature of version 2.1.1 of GlobalPlatform Card Specification. The following table lists all the impacts of this new feature. Impacts are classified in a sequential order that reflects the Card Specification index.

Version 2.1.1 section number	Description
Section 5.2.1.2	Executable Load File Life Cycle
Section 6.4.2.3	New section: Executable Load File and related Application Removal
Section 7.6.4	New Delegated Deletion option
Section 9	New entry in Table 9-1 for combined deletion
Section 9.2.1	New feature of DELETE command
Sections 9.2.2, 9.2.2.2	New value for parameter P2 of DELETE command
Section 9.2.2.3	Command data contents for DELETE command

5. Enhanced C-MAC

The enhanced C-MAC is a new recommended feature of version 2.1.1 of GlobalPlatform Card Specification. The following table lists all the impacts of this new feature on both Secure Channel Protocol '01' (SCP 01) and Secure Channel Protocol '02' (SCP 02). Impacts are classified in a sequential order that reflects the Card Specification index.

Version 2.1.1 section number	Description
Appendix D.1.1	New implementation option 'i' for SCP 01
Appendix D.1.3	Message Integrity in SCP 01
Appendix D.1.5	New ICV Encryption for SCP 01
Appendix D.3.3	SCP 01 C-MAC generation and verification
Appendix E.1.1	New implementation options 'i' for SCP 02
Appendix E.1.3	Message Integrity in SCP 02
Appendix E.3.4	New ICV Encryption for SCP 02
Appendix E.4.4	SCP 02 C-MAC generation and verification

6. Miscellaneous

The following table lists few miscellaneous enhancements of version 2.1.1 of GlobalPlatform Card Specification. They are classified in a sequential order that reflects the Card Specification index.

Version 2.1.1 section number	Description
Section 1.2, Appendix A.2	Reference to Java Card 2.2 specifications
Sections 1.3, 1.4	Terminology and abbreviations updates
Section 9.3.2.2	Receipt Confirmation Counter retrieval with GET DATA command
Sections 9.4.2.2, 9.4.3.1	TLV format for GET STATUS response