



GlobalPlatform Card v2.1.1 to v2.2 Mapping Guidelines

Of Existing 2.1.1 Implementations

Version 1.0

Table of contents

1. OVERVIEW

- 1.1. SECURITY DOMAINS
- 1.2. RECOMMENDED PRIVILEGES
- 1.3. RECOMMENDED APPLICATION PROGRAMMING INTERFACES
 - 1.3.1. *GlobalPlatform 2.2*
 - 1.3.2. *Java Card*
- 1.4. CLARIFICATIONS FOR JAVA CARD AND EMV

2. SECURITY PRINCIPLES

- 2.1. PRIVILEGES
- 2.2. ISSUER SECURITY DOMAIN
- 2.3. SUPPLEMENTARY SECURITY DOMAINS PRESENT ON AN IMPLEMENTATION
- 2.4. APPLICATIONS

3. DATA RECOMMENDATIONS

- 3.1. OPEN
- 3.2. ISSUER SECURITY DOMAIN
 - 3.2.1. *Data Store*
 - 3.2.2. *Secure Channel Keys*
 - 3.2.3. *Default Secure Channel Sequence Counter (tag 'C1')*
 - 3.2.4. *Key Information Template and Key Information Data (tags 'E0' and 'C0')*
- 3.3. SUPPLEMENTARY SECURITY DOMAINS PRESENT ON THE IMPLEMENTATIONS
 - 3.3.1. *Data Store*
 - 3.3.2. *Secure Channel Keys*
 - 3.3.3. *DAP Verification Key*
 - 3.3.4. *Default Secure Channel Sequence Counter (tag 'C1')*
 - 3.3.5. *Key Information Template and Key Information Data (tags 'E0' and 'C0')*
- 3.4. CVM INTERFACE

4. KEY USAGE

5. SECURE CHANNEL

- 5.1. DATA FIELD DECRYPTION
- 5.2. MAC VERIFICATION
- 5.3. DECRYPTION USING DEK
- 5.4. CARD CHALLENGE

6. APDU COMMANDS

- 6.1. DELETE
 - 6.1.1. *Definition*
 - 6.1.2. *Recommendations*
- 6.2. EXTERNAL AUTHENTICATE
 - 6.2.1. *Definition*
 - 6.2.2. *Recommendations*
- 6.3. GET DATA
 - 6.3.1. *Definition*
 - 6.3.2. *Recommendations*
- 6.4. GET STATUS

- 6.4.1. *Definition*
- 6.4.2. *Recommendations*
- 6.5. INITIALIZE UPDATE
 - 6.5.1. *Definition*
 - 6.5.2. *Recommendations*
- 6.6. INSTALL
 - 6.6.1. *Definition*
 - 6.6.2. *Recommendations*
- 6.7. LOAD
 - 6.7.1. *Definition*
 - 6.7.2. *Recommendations*
- 6.8. MANAGE CHANNEL
 - 6.8.1. *Definition*
 - 6.8.2. *OPEN Recommendations*
- 6.9. PUT KEY (DES KEYS)
 - 6.9.1. *Definition*
 - 6.9.2. *Recommendations*
- 6.10. PUT KEY (RSA PUBLIC KEY)
 - 6.10.1. *Definition*
 - 6.10.2. *Recommendations*
- 6.11. SELECT
 - 6.11.1. *Definition*
 - 6.11.2. *OPEN Recommendations*
 - 6.11.3. *Security Domain Recommendations*
- 6.12. SET STATUS
 - 6.12.1. *Definition*
 - 6.12.2. *Recommendations*
- 6.13. STORE DATA
 - 6.13.1. *Definition*
 - 6.13.2. *Recommendations*
- 6.14. RESPONSE CODES

7. APPLICATION PROGRAMMING INTERFACE

- 7.1. CLASS GPSSYSTEM
 - 7.1.1. *byte getCardContentState()*
 - 7.1.2. *byte getCardState()*
 - 7.1.3. *CVM getCVM(byte bcVMIdentifier)*
 - 7.1.4. *GPREgistryEntry getRegistryEntry(AID reqAID)*
 - 7.1.5. *SecureChannel getSecureChannel()*
 - 7.1.6. *GlobalService getService(AID serverAID, short sServiceName)*
 - 7.1.7. *boolean lockCard()*
 - 7.1.8. *boolean terminateCard()*
 - 7.1.9. *boolean setATRHistBytes(byte[] baBuffer, short sOffset, byte bLength)*
 - 7.1.10. *boolean setCardContentState(byte bState)*
- 7.2. INTERFACE SECURECHANNEL
 - 7.2.1. *short processSecurity(apdu)*
 - 7.2.2. *Processing for Intialize Update command*
 - 7.2.3. *Processing for External Authenticate command*

- 7.2.4. *short wrap (byte[] baBuffer, short sOffset, short sLength)*
- 7.2.5. *short unwrap (byte[] baBuffer, short sOffset, short sLength)*
- 7.2.6. *short decryptData (byte[] baBuffer, short sOffset, short sLength)*
- 7.2.7. *short encryptData (byte[] baBuffer, short sOffset, short sLength)*
- 7.2.8. *void resetSecurity()*
- 7.2.9. *byte getSecurityLevel()*

7.3. INTERFACE CVM

- 7.3.1. *boolean isActive()*
- 7.3.2. *boolean isSubmitted()*
- 7.3.3. *boolean isVerified()*
- 7.3.4. *boolean isBlocked()*
- 7.3.5. *byte getTriesRemaining()*
- 7.3.6. *boolean update(byte[] baBuffer, short sOffset, byte bLength, byte bFormat)*
- 7.3.7. *boolean resetState()*
- 7.3.8. *boolean blockState()*
- 7.3.9. *boolean resetAndUnblockState()*
- 7.3.10. *boolean setTryLimit (byte bTryLimit)*
- 7.3.11. *short verify(byte[] baBuffer, short sOffset, byte bLength, byte bFormat)*

7.4. INTERFACE GPREGISTRYENTRY

- 7.4.1. *void deregisterService(short sServiceName)*
- 7.4.2. *AID getAID()*
- 7.4.3. *short getPrivileges(byte baBuffer, short sOffset)*
- 7.4.4. *byte getState()*
- 7.4.5. *boolean isAssociated(AID SDAID)*
- 7.4.6. *boolean isPrivileged(byte bPrivilege)*
- 7.4.7. *void registerService(short sServiceName)*
- 7.4.8. *boolean setState(byte bState)*

7.5. INTERFACE SECURECHANNELX

- 7.5.1. *void setSecurityLevel(byte bSecurityLevel)*

8. APIS SPECIFIC RECOMMENDATIONS

- 8.1.1. *Processing for External Authenticate command*
- 8.1.2. *CVM getCVM(byte bCVMIIdentifier)*

9. LIST OF TABLES