GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

GlobalPlatform Card
Confidential Card Content Management
Card Specification v2.2 - Amendment A

Version 1.0.1

Public Release

January 2011

Document Reference: GPC_SPE_007

Table of contents

1 Normative References

Standard / Specification	Description	Ref
GlobalPlatform Card Specification v2.2.1	Card Specification v2.2.1 from GlobalPlatform	[0]
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	[1]
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	[2]
GlobalPlatform Systems Scripting Language Specification	GlobalPlatform Systems Scripting Language Specification, version 1.1.0	[3]
PKCS#1	PKCS #1 v2.1: RSA Cryptography Standard, *RSA Laboratories*, June 14, 2002	[4]
ISO/IEC 7816-4:2005	Identification cards – Integrated circuit(s) cards - Part 4: Organization, security and commands for interchange	[5]

Table 1: Normative References

1.1 Revision History

Version 1 of this document was published in October 2007. Subsequently, errata and precisions on this document were developed and published.

Version 1.0.1 of this document incorporates the contents of "Errata and Precisions for GlobalPlatform Card Specification Amendment A v1.0" as well as errata and precisions made during the development of the UICC Configuration v1.0 and v1.0.1.

The contents of sections 4.8 and 4.9 are now integrated in to GlobalPlatform Card Specification v2.2.1.

2 Abbreviations and Notations

Abbreviation	Meaning
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
APSD	Application Provider Security Domain
AUT	AUThentication
CA	Controlling Authority
CASD	Controlling Authority Security Domain
CCT	Cryptographic Checksum Template
CT	Confidential Template
ISD	Issuer Security Domain
KAT	Key Agreement Template
KS	Secret Key of a symmetric scheme
LPO	Link Platform Operator
MAC	Message Authentication Code
OTA	Over-The-Air
PK	Public Key of an asymmetric key pair.
PKI	Public Key Infrastructure
SK	Private key of an asymmetric key pair
CERT.AP.AUT	Application Provider Certificate holding a Public Key suitable for Signature Verification
CERT.AP.CT	Application Provider Certificate holding a Public Key suitable for Encryption
CERT.CASD.AUT	CASD Certificate holding a Public Key suitable for Signature Verification
CERT.CAST.CT	CASD Certificate holding a Public Key suitable for Encryption
KS.AP.CT	Application Provider Symmetric Key used for Encryption/Decryption
KS.CASD.AUT	CASD Symmetric Key used for Signature/Verification
KS.CASD.CT	CASD Symmetric Key used for Encryption/Decryption
PK.AP.AUT	Application Provider Public Key used for Signature Verification
PK.AP.CT	Application Provider Public Key used for Encryption
PK.CA.AUT	CA Public Key used to verify certificates
PK.CASD.AUT	CASD Public Key used for Signature Verification
PK.CASD.CT	CASD Public Key used for Encryption

Abbreviation	Meaning
SK.CA.AUT	CA Private Key used to sign certificates (off-card)
SK.CASD.AUT	CASD Private Key used for Signature
SK.CASD.CT	CASD Private Key used for Decryption

Table 2: Abbreviations and Notations

3 Confidential Application Loading

3.1 Scope of the document

This document defines a mechanism for an Application Provider to confidentially manage its application i.e. to load, install and personalize using a third party communication network. This third party shall not be able to access to clear text of any confidential data and code belonging to the Application Provider. The network may provide or not its own additional security and confidentiality means. The entity representing this link could be a Link Platform Operator (LPO) such as an Over-The-Air platform operator compliant with ETSI specification TS 102 225 [1] and TS 102 226 [2] e.g. a Mobile Network Operator.

This document describes:

- New Data Grouping Identifiers to authenticate the Application Provider through a secret key or its certificate.
- New Data Grouping Identifiers and Store Data command parameter's value to generate on-card the necessary keys.
- New Data Grouping Identifiers and Store Data command parameter's value to push the necessary keys on-card.
- A mechanism to derive the necessary keys from the on-card generated key.
- New tag for encrypted Load File Data Block.
- A generation mechanism based on symmetric key for Delegated Management Tokens: signatures of one or more Delegated Management functions (loading, installing, extraditing and deleting).
- New API for confidential personalization.
- New APIs to secure on-card key generation.

3.2 Use Cases and Requirements

This document proposes a specification addendum to support the following requirements:

- An Application Provider shall be able to load confidential applications using an untrusted transport link to protect its assets.
- A Link Platform Operator (LPO) shall be able to create on-card component to load and manage confidential application and transfer the ownership to an Application Provider.
- An Application Provider shall be able to instantiate its own applications and to personalize them.

Security Domains are responsible of the on-card application management and so are the candidates to realize those requirements. Thus the Application Provider uses a Security Domain (APSD) to manage confidential loading:

- The keys used by the APSD shall not be known by the LPO. To achieve this, an on-card controlling entity (extended role of a Controlling Authority) shall be able to secure the key creation of the APSD.
- This controlling entity shall be able to secure the APSD personalization.
- The APSD shall be personalized using the LPO network.

Additionally it is required that:

- It shall be possible to support confidential loading on non-PK card.
- The specification modifications will not require modifications to the current loading mechanism (format of commands remain unchanged) to avoid modifying existing OTA infrastructure

- It shall be possible to support AP Application personalization. The content of the data being personalized is beyond the scope of this specification

4 Specification Amendments

This section defines the APDU commands and the Data Grouping Identifiers to be submitted to the card in order to personalize the Controlling Authority and the Application Provider Security Domains.

Two schemes are defined to personalize the Application Provider Security Domain

1. Pushing mandatory data: Security Domain keys are sent to the Application Provider Security Domain. Asymmetric cryptographic scheme shall be used.
2. Pulling mandatory data: Security Domain keys are generated on-card and then returned to the Application Provider. Asymmetric or Symmetric cryptographic scheme could be used

It defines the commands and the Data Grouping Identifiers to submit to the card in order

- To verify the Application Provider certificate and cryptogram.
- To describe the key derivation data and algorithm to either generate keys on the card or to describe the pushed keys.

It also defines new Tokens for Delegated Management and a new tag for encrypted Load File Data Block.

4.1 DGI for Personalizing the Security Domain Mandatory Data

This section defines the command and DGI to be submitted to the Security Domain to personalize it with the mandatory set of data for:

1. The Controlling Authority Security Domain (CASD).
2. The Application Provider Security Domain (APSD).

The STORE DATA command is used to personalize the Security Domain. The Data Group Identifier for a Security Domain mandatory data is defined in Table 3.

The structure of the DGI is specified in Annex B of the GP Systems Scripting Language Specification[3].

DGI	Data Content	Function	Encrypt
'0070'	Variable	One or more TLV coded objects	No

Table 3: Data Grouping Identifiers for Personalizing the APSD and CASD

The data object tags defined in section 11.3.2.1 of GP221[0] shall be used to populate DGI '0070'.

4.2 Public key certificates and DES signature

The STORE DATA command can be used in both scenarios – and shall be coded as a case 3 command:

1. Personalization of the CASD Public Key Certificate.
2. Verification of the Application Provider Public Key Certificate.

4.2.1 DGI for Controlling Authority Certificate

Personalization of the Controlling Authority Security Domain (i.e. the CASD Public Key Certificate) may take place during pre-issuance or post-issuance. The Data Group Identifier for CASD Public Key Certificate is defined in Table 4.

DGI	DGI Length	Data Content	Function	Encrypt
'7F21'	Variable	Certificate	Controlling Authority Public Key Certificate	No

Table 4: Data Grouping Identifier for Controlling Authority Certificate

4.2.2 DGI for the Application Provider Certificate

The Controlling Authority generates the Application Provider Public Key Certificate. When the APSD receives the certificate, it uses the `Authority` interface to request the CASD to verify the Application Provider Public Key Certificate. The DGI value of '00AE' is an input template for verification of a certificate. The DGI value of '00DE' is introduced to distinguish between certificates with and without message recovery.

The Data Group Identifiers for Application Provider Certificate is defined in Table 5.

DGI	DGI Length	Data Content	Function	Encrypt
'00AE'	Variable	Certificate without message recovery	Application Provider Public Key Certificate	No
'00DE'	Variable	Certificate with message recovery	Application Provider Public Key Certificate	No

Table 5: Data Grouping Identifiers for Application Provider Certificate

The DGIs for the Application Provider Public Key Certificate are formatted as described in Table 7.

The Application Provider Public Key Certificate may be itself encrypted. To support this scenario, the CASD shall be personalized with an asymmetric Private Key for confidentiality: SK.CASD.CT, to decrypt the AP certificate and with the corresponding Public Key Certificate: CERT.CASD.CT that may be retrieved by the Application Provider. The Application Provider Public Key Certificate is then encrypted off-card with the Controlling Authority Security Domain Confidentiality Public Key: PK.CASD.CT. The Data Group Identifiers for encrypted Application Provider Certificate are defined in Table 6.

DGI	DGI Length	Data Content	Function	Encrypt
'80AE'	Variable	Encrypted certificate (certificate without message recovery)	Encrypted Application Provider Public Key Certificate	Yes
'80DE'	Variable	Encrypted certificate (certificate with message recovery)	Encrypted Application Provider Public Key Certificate	Yes

Table 6: Data Grouping Identifiers for Encrypted Application Provider Certificate

The DGIs '80AE' or '80DE' contain the (non-TLV coded) cryptogram value of the encrypted Application Provider Public Key Certificate. Once decrypted by the Controlling Authority Security Domain Confidentiality Private Key: SK.CASD.CT, the Application Provider Public Key Certificate is formatted as described in Table 7.

4.2.3 Content of the DGI

When using asymmetric Controlling Authority keys, the content of DGIs '7F21', '00AE'/'00DE' and '80AE'/'80DE' is one (or more) certificate(s) coded in TLV format with a tag value of '7F21'. There may be more than one certificate if chains of certificates are supported by the implementation scheme.

Table 7 describes the content of the DGI '7F21'.

Tag	Length	Data Element	Presence
'7F21'	'00' - '7F' or '81 80' - '81 FF' or '82 01 00' - '82 FF FF'	Certificate data, as described in section F.1.2.4 of GP221[0]	Mandatory
'7F21'	'00' - '7F' or '81 80' - '81 FF' or '82 01 00' - '82 FF FF'	Certificate data, as described in section F.1.2.4 of GP221[0]	Optional
…	…	…	…

Table 7: Data Content for DGI '7F21'

Table 8 describes the coding of the DGI's content for the public key certificates and DES signature.

Tag	Length	Data Element	Presence
'7F21'	'00' - '7F' or '81 80' - '81 FF' or '82 01 00' - '82 FF FF'	Certificate data, as described in section F.1.2.4 of GP221[0]	Conditional
'8E'	Variable	MAC (symmetric cryptography)	Conditional

Table 8: Data Content for DGI '00AE', '00DE', '80AE' or '80DE'

When using symmetric Controlling Authority keys, there is no Controlling Authority Public Key Certificate to personalize (no DGI '7F21') and the content of DGI '00AE' is the Application Provider encryption Key, KS.AP.CT, signed by the Controlling Authority coded in TLV format with a tag value of '8E' (ISO tag value for cryptographic checksum).

After the content of DGI '00AE', '80AE', '00DE', or '80DE' is successfully verified and validated the Application Provider key (PK.AP.CT, PK.AP.AUT, or KS.AP.CT) contained in the DGI is ready for use.

4.3 Pull Model: DGI Application Provider Off-card Entity Key

The Pull Model requires that the APSD is provided with the Application Provider Public Key (or Symmetric Key) for confidentiality PK.AP.CT (or KS.AP.CT). This key is used to encrypt the Secure Channel keys generated on-card.

A specific DGI will allow the support of both symmetric and asymmetric cryptography, with both certificates with and without message recovery, such as:

- The Application Provider Key is asymmetric (PK.AP.CT). The Controlling Authority provides certificates with message recovery (DGI = '00DE'). The CASD verifies the Application Provider Key certificate with PK.CA.AUT and retrieves PK.AP.CT from the certificate.

- The Application Provider Key is asymmetric (PK.AP.CT). The Controlling Authority provides certificates without message recovery (DGI = '00AE'). The CASD verifies the Application Provider Key certificate with PK.CA.AUT. The PK.AP.CT is provided encrypted in a separate DGI since the certificate is without message recovery.
- The Application Provider Key is symmetric (KS.AP.CT) and encrypted with the symmetric Controlling Authority Key (KS.CA.CT).

The Data Group Identifier for Application Provider Key CRT is defined in Table 9 – the STORE DATA command shall be coded as a Case 3 command.

DGI	DGI Length	Data Content	Function	Encrypt
'00B8'	Variable	Control Reference Template for confidentiality (CT)	Application Provider Key information data	No

Table 9: Data Grouping Identifier for Application Provider Key CRT

Furthermore, the Application Provider Key is used to encrypt data and keys sent in responses from the Application Provider Security Domain (not in commands sent to APSD). Leveraging the Key Usage Qualifier values described in section F.3.1.2 of GP221[0] the data content for the Application Provider Key DGI is defined in Table 10.

Tag	Length	Data Element	Presence
'B8'	Variable	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier = '40' (encipherment of sensitive data in responses)	Mandatory
'80'	'01'	Key Type according GP221[0] Table 11-16	Mandatory
'81'	'01' or '02'	Key Length	Mandatory
'82'	'01'	Key Identifier = '00' - '7F'	Optional
'83'	'01'	Key Version Number = '01' - '7F'	Optional
'B8'	Variable	CRT tag (CT)	Conditional
…	…	…	…

Table 10: Data Content for DGI '00B8'

Segregating encrypted and non-encrypted DGIs requires a DGI for the encrypted Application Provider Key, either symmetric: KS.AP.CT or asymmetric: PK.AP.CT. The Data Grouping Identifier for encrypted Application Provider Key is defined in Table 11.

DGI	DGI Length	Data Content	Function	Encrypt
'80B8'	Variable	Encrypted key	Encrypted Application Provider Key	Yes

Table 11: Data Grouping Identifier for encrypted Application Provider Key

The DGI '80B8' contains the (non-TLV coded) cryptogram value of the encrypted Application Provider Key: KS.AP.CT or PK.AP.CT.

4.4 DGI for Security Domain Symmetric Key

The DGI '00A6' is used as content in the STORE DATA command either:

1. To trigger the on-card Security Domain key generation for the Pull Model,
2. To describe the keys contained in the DGI '8010' (see section 4.5) for the Push Model.

The format of the STORE DATA command data is DGI. The Data Group Identifier for key generation is defined in Table 12.

DGI	DGI Length	Data Content	Function	Encrypt
'00A6'	Variable	Control Reference Template (KAT)	Key agreement/generation CRT	No

Table 12: Data Grouping Identifier for Key Generation

The data content for DGI '00A6' is defined in Table 13.

Tag	Length	Data Element	Presence
'A6'	Variable	CRT tag (KAT)	Mandatory
'90'	'01'	Scenario Identifier: '00' – '2F': Reserved for GlobalPlatform Use (e.g. Configurations) '30' – '9F': RFU 'A0' – 'BF': Reserved for Proprietary Use 'C0' – 'FF': RFU	Mandatory
'95'	'01'	Key Usage Qualifier = '5C' (1 secure channel base key) or '10' (3 secure channel keys) (see GP221[0] Table 11-17)	Mandatory
'96'	'01'	Key Access according to GP221[0] Table 11-18	Optional
'80'	'01'	Key Type according to GP221[0] Table 11-16	Mandatory
'81'	'01' or '02'	Key Length	Mandatory
'82'	'01'	Key Identifier = '00' - '7F'	Optional
'83'	'01'	Key Version Number = '01' - '7F'	Optional
'91'	'00', '02', '05', or '08'	Initial value of sequence counter	Optional
'45'	1-n	Security Domain Image Number (SDIN)	Optional

Table 13: Data Content for DGI '00A6' – Master Key CRT

The value of tag '90' (Scenario Identifier) allows the Security Domain to decide a course of action when receiving tag 'A6' (e.g. triggering on-card key generation or waiting for other DGI containing keys). Using the Pull Model, an ISO/IEC 7816-4 [5] Case 4 type STORE DATA command as described in section 5.1 shall be sent to trigger on-card key generation and to retrieve the generated data.

When the Key Access field is not present, the default key access value is '00'.

If the Scenario Identifier indicates that the STORE DATA command is used to trigger Security Domain key generation, then the following steps shall occur:

- A key with type and length provided in the CRT shall randomly be generated (RGK).
- The RGK shall be encrypted with the Application Provider public key or the Application Provider symmetric key (PK.AP.CT or KS.AP.CT)
- The encrypted RGK shall be concatenated with the AID of the Security Domain and the Application Provider ID and the SIN.
- The partially encrypted message is signed by the on-card CASD private key using the `Authority` interface.
- The signed message and the on-card CASD certificate shall be returned as part of the STORE DATA response.

If the key usage qualifier within the CRT is '10' then a secure channel key set with 3 keys known as K_{ENC}, K_{MAC} and K_{DEK} of the same type and length as provided in the CRT shall be derived from the RGK using the key data and the key derivation algorithm defined respectively in sections 4.6.1 and 4.6.2.

If the key identifier is present in the CRT then the identifier of the derived K_{ENC} shall be set to this value. The key identifier of the derived K_{MAC} shall be set to the key identifier provided in the CRT incremented by 1. The key identifier of the derived K_{DEK} shall be set to the key identifier provided in the CRT incremented by 2.

If the key version is present in the CRT then the version of the key set shall be set to this value.

If the initial value of the sequence counter is present in the CRT then the initial value of the sequence counter for the key set shall be set to this value.

If the optional data elements are not present in the CRT the default values shall be:

- The key identifier is '01' for the K_{ENC}, '02' for the K_{MAC}, and '03' for the K_{DEK}.
- The key version is '01' for the key set.
- The initial value of the sequence counter is 0 for the key set.

The Security Domain Key generation DGI is generalized to support generation of not only the Master Key: RKG, but also of all Secure Channel keys: C-ENC, C-MAC and C-DEK. The data content for DGI '00A6' is defined in Table 14.

Tag	Length	Data Element	Presence
'B8'	Variable	CRT tag (CT)	Conditional
'95'	'01'	Key Usage Qualifier = '18' (secure messaging for commands: S-ENC)	Mandatory
'80'	'01'	Key Type according GP221[0] Table 11-16	Mandatory
'81'	'01' or '02'	Key Length	Mandatory
'82'	'01'	Key Identifier = '00' - '7F'	Optional
'83'	'01'	Key Version Number = '01' - '7F'	Optional
'91'	'00' or '08'	Initial value of sequence counter	Optional
'45'	1-n	Security Domain Image Number	Optional
'B4'	Variable	CRT tag (CCT)	Mandatory
'95'	'01'	Key Usage Qualifier = '14' (secure messaging for commands: S-MAC)	Mandatory
'80'	'01'	Key Type according GP221[0] Table 11-16	Mandatory
'81'	'01' or '02'	Key Length	Mandatory
'82'	'01'	Key Identifier = '00' - '7F'	Optional
'83'	'01'	Key Version Number = '01' - '7F'	Optional
'91'	'00' or '08'	Initial value of sequence counter	Optional
'45'	1-n	Security Domain Image Number	Optional
'B8'	Variable	CRT tag (CT)	Conditional
'95'	'01'	Key Usage Qualifier = '48' (secure messaging for commands: DEK)	Mandatory
'80'	'01'	Key Type according GP221[0] Table 11-16	Mandatory
'81'	'01' or '02'	Key Length	Mandatory
'82'	'01'	Key Identifier = '00' - '7F'	Optional
'83'	'01'	Key Version Number = '01' - '7F'	Optional
'91'	'00' or '08'	Initial value of sequence counter	Optional
'45'	1-n	Security Domain Image Number	Optional

Table 14: Data Content for DGI '00A6' – Secure Channel Keys CRT

4.5 Push Model: DGI for Secure Channel Symmetric Keys

DGI '8010' contains the encrypted symmetric keys and immediately follows the DGI '00A6' which provides the description of the keys.

DGI	DGI Length	Data Content	Function	Encrypt
'8010'	Variable	Encrypted Secure channel symmetric keys	Application provider symmetric secure channel keys	Yes

Table 15: Data Grouping Identifier for Encrypted Secure Channel Keys

The underlying plain text structure is provided in Tables 15 and 16. If the asymmetric scheme is used, the data content is ciphered using the PK.CASD.CT key with the encryption scheme RSAES-PKCS-V1.5 as specified in PKCS#1[4]. The length of each key is provided by the value of the CRT tag '81' within the DGI '00A6'. If the symmetric scheme is used, the data content is ciphered in CBC mode and the ICV is set to zero using KS.CASD.CT. If the plain text data is not a multiple of the encryption block length the last block shall be filled with arbitrary padding bytes.

If the DGI '00A6' indicates three Keys the Data content is as in Table 16.

Data Element	Presence
ENC key	Mandatory
MAC key	Mandatory
DEK key	Mandatory

Table 16: Data Content for DGI '8010' – Encrypted Secure Channel Keys Values

If the DGI '00A6' indicates one Master Key, then the data content defined in Table 17.

Data Element	Presence
Master key	Mandatory

Table 17: Data Content for DGI '8010' – Master Key Value

4.6 Static Key Generation for Secure Channel Protocol '02' with 3 Secure Channel Keys

When bit 1 of the SCP02 implementation option is set to '1', the SCP uses three Secure Channel keys.

4.6.1 Key Data

The Key Data is generally used for diversification of derived keys when they are all generated from the same Master Key. Since in this case the on Security Domain key is generated using random there is no need for a diversification data. Therefore the six bytes of binary '1' i.e. 'FF FF FF FF FF FF' is used to derive the Key Set from the random generated key.

4.6.2 Key Derivation Algorithm

This section defines the algorithm to derive the three static keys of the Secure Channel Key Set from Master Key randomly generated.

The K_{ENC} is a 16-byte (112 bits plus parity) DES key. The K_{ENC} will be derived in the following way:

K_{ENC} := DES3(RGK)['FF FF FF FF FF FF' || 'F0' || '01'] ||
DES3(RGK)['FF FF FF FF FF FF' || '0F' || '01']

The K_{MAC} is a 16-byte (112 bits plus parity) DES key The K_{MAC} will be derived in the following way:

K_{MAC} := DES3(RGK)['FF FF FF FF FF FF' || 'F0' || '02'] ||
DES3(RGK)['FF FF FF FF FF FF' || '0F' || '02']

The K_{DEK} is a 16-byte (112 bits plus parity) DES key. The K_{DEK} will be derived in the following way:

K_{DEK} := DES3(RGK)['FF FF FF FF FF FF' || 'F0' || '03'] ||
DES3(RGK)['FF FF FF FF FF FF' || '0F' || '03']

4.7 Introduction of a Token Using Symmetric Keys

The token calculation described in Annex C4 of the GlobalPlatform Card Specification v2.2 is replaced by the following text in order to introduce a DES load Token using Symmetric Key and a PKCS load token.

C.4 Load Token

Tokens are signatures, generated by the Card Issuer. Tokens are the proof that the Card Issuer has authorized the Card Content Management operation being performed. Tokens are generated and verified according to this appendix. Tokens may be generated for use on multiple cards, depending on the Card Issuer's security policy.

C.4.1 PKCS Scheme

A PKCS token is an RSA signature, being the decryption (with the token private key) of the SHA-1 message digest of the appropriate data. The signature scheme for tokens is as defined in Annex B.3- *Public Key Cryptography Scheme 1 (PKCS#1)*.

C.4.2 DES TOKEN

A DES token is a signature of appropriate data. This signature is a MAC of the appropriate data according to appendix B.1.2.2 - *Single DES plus Final Triple DES*. Padding of the data is as defined in appendix B.4 - *DES Padding*.

…/……/…

4.8 Ciphered Load File

A new tag, 'D4', is introduced to send a Ciphered Load File Data Block in the LOAD command as defined in section 11.6.2.3 of GP221[0].The encryption mechanism for the Ciphered Load File Data Block will be based on:

- Encryption algorithm corresponding to the key type coding of encryption key (i.e. RSA, DES, AES see section 11.1.8 of GP221[0] - Key Type Coding).
- For Symmetric algorithm, the padding is as specified in Annex B.4 of GP221[0].

The associated Security Domain performs the decryption of the Ciphered Load File Data block.

Note: To be consistent with the DAP key, the encryption key shall be defined in a configuration.

The padding of the Load File Data Block could be computed using the length indicated by the value of tag 'D4' (length of the encrypted load file) and the length indicated inside the load file itself.

4.9 Ciphered Load File Data Block Privilege

A new privilege, the Ciphered Load File Data Block privilege is introduced. See GP221[0] in section 9.1.3.7, Table 6-1, section 9.3.5 and Table 11-9.

4.10 DGI for Personalizing Security Domain Keys

The encryption and decryption of the DGI's content shall be performed using the Data Encryption session key (DEK session key) and the algorithm supported by the Secure Channel Protocol for sensitive data encryption/decryption.

All encrypted data grouping content defined in this section shall be padded with as many arbitrary bytes as needed to reach the required block size (depending on the algorithm used by the DEK session key), e.g. 8 bytes for DES encryption, 16 bytes for AES encryption.

The STORE DATA command shall be coded as a Case 3 command. Each DGI described in the following sections should be sent in a single STORE DATA command, i.e. a DGI should not be split over multiple APDUs.

The Data Group Identifier for the Key Control Reference Template is defined in Table 18:

DGI	DGI Length	Data Content	Encrypt
'00B9'	Var	Key Information Data	No

Table 18: DGI for Key Information Data

4.10.1 Asymmetric Key Scheme

When supporting an asymmetric scheme, either the Data Grouping Identifier's '8112' Private Key Exponent, or the Data Grouping Identifiers '8121' to '8125' RSA Chinese Remainder Theorem (RSACRT) constants shall be used to load/update the private component.

The DGI '0011' is used for the Public Key Exponent. The DGI '0010' is used for the Modulus.

The key data format is:

1. Most significant byte first
2. Fixed length related to the length of the modulus, zero-padding to the left.
3. Exception for the public key exponent which is encoded using the shortest byte representation.
4. When ciphering a key component value additional padding shall be added according to the encryption algorithm used.

The Control Reference Template is used to describe the keys sent in commands and responses to or from the Security Domains.

4.10.1.1. DGIs for the RSA Public Key

The data content of the DGI for the Key Control Reference Template for the asymmetric key scheme is defined in Table 19:

Tag	Length	Description	Presence
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A1' Key Modulus	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Optional
'B9'	Var	CRT tag (CT)	Conditional
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A0' Public Key Exponent	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory

Table 19: Data Content for DGI '00B9' – RSA Public Key

The following Data Grouping Identifiers are used to populate the Key Modulus and Public Key Exponent and should immediately follow DGI '00B9':

DGI	Length	Data Content	Encrypt
'0010'	Var	Key Modulus	No
'0011'	Var	Public Key Exponent	No

Table 20: Data Content for DGIs '0010' and '0011'

4.10.1.2. DGIs for the RSA Private Key, Exponent Format

When the private key exponent format is used to populate asymmetric keys, the following data content shall be included in the DGI '00B9':

Tag	Length	Description	Presence
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A1' Key Modulus	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Optional
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A3' Private Key Exponent	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory

Table 21: Data Content for DGI '00B9' – RSA Private Key, Exponent Format

The following Data Grouping Identifiers are used to populate the Private Key when the private key exponent format is used:

DGI	Length	Data Content	Encrypt
'0010'	Var	Key Modulus	No
'8112'	Var	Private Key Exponent	Yes

Table 22: Data Content for DGIs '0010' and '8112'

DGI '8112' shall follow DGI '00B9'.

4.10.1.3. DGIs for the RSA Private Key, CRT Format

When the Chinese Remainder Theorem (CRT) format is used to populate the RSA asymmetric keys, the following data content shall be included in DGI '00B9':

Tag	Length	Description	Presence
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A6' Private Key q^{-1} mod p	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory
'B9'	Var	CRT tag (CT)	Mandatory

Tag	Length	Description	Presence
'95'	'01'	Key Usage Qualifier values according to section 1.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A8' Private Key *d* mod (*q* – 1)	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A7' Private Key *d* mod (*p* – 1)	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A5' Private Key prime factor *q*	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'80'	'01'	Key Type = 'A4' Private Key prime factor *p*	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory

Table 23: Data Content for DGI '00B9' – RSA Private Key, CRT Format

The following Data Grouping Identifiers are used to populate the Private Key when the Chinese Remainder Theorem format is used:

DGI	Length	Data Content	Encrypt
'8121'	Var	RSACRT constant q^{-1} mod *p*	Yes
'8122'	Var	RSACRT constant *d* mod (*q* – 1)	Yes
'8123'	Var	RSACRT constant *d* mod (*p* – 1)	Yes

DGI	Length	Data Content	Encrypt
'8124'	Var	RSACRT constant prime factor *q*	Yes
'8125'	Var	RSACRT constant prime factor *p*	Yes

Table 24: Data Content for DGIs '8121' through '8125'

These DGIs shall follow DGI '00B9'.

4.10.2 Symmetric Key Scheme

When supporting a symmetric scheme, the Data Grouping Identifiers '00B9' and '8113' shall be used to load/update a secret key.

The key data format is:

1. Most significant byte first
2. When ciphering a key component value additional padding shall be added according to the encryption algorithm used.

The CRT defined in Table 25, below, is used to describe the symmetric keys sent in responses/commands from/to the Security Domains.

Tag	Length	Description	Presence
'B9'	Var	CRT tag (CT)	Mandatory
'95'	'01'	Key Usage Qualifier values according to section 11.1.9 of GP221[0]	Mandatory
'96'	'01	Key Access according to GP221[0] Table 11-18	Optional
'80'	'01'	Key Type according to GP221[0] Table 11-16	Mandatory
'81'	'01' or '02'	Key Length, in bytes (unsigned integer value)	Mandatory
'82'	'01'	Key Identifier	Mandatory
'83'	'01'	Key Version Number	Mandatory
'84'	'03'	Key check value	Mandatory
'B9'	'Var'	CRT tag (CT)	Conditional
…	…	…	…

Table 25: Data Content for DGI '00B9' – Symmetric Scheme

When the Key Access field is not present, the default Key Access value is '00'.

The decrypted key shall be verified against its associated check value as described in section B.5 of GP221[0]. If this comparison fails, a response of '6982' shall be returned.

4.10.2.1. DGI for a Symmetric Scheme in Secret Key Format

The following Data Grouping Identifier is used to populate a secret key:

DGI	Length	Data Content	Encrypt
'8113'	Var – multiple of 8	Secret Key	Yes

Table 26: Data Content for DGI '8113'

DGI '8113' shall immediately follow DGI '00B9' and shall be repeated once for each key described in DGI '00B9'.

5 API for Confidential Personalization

Two interfaces are needed to support the confidential application personalization. These interfaces are the `Personalization` and `Authority` interfaces and are added into the `org.globalplatform` package. See GlobalPlatform Java Card™ API v1.2.

5.1 `Personalization` Interface

Application personalization is defined in section 7.3.3 of GP221[0] – Personalization. In certain situations the Applet needs to send response data during personalization. For this purpose, the new interface `org.globalplatform.Personalization` is introduced. The Associated Security Domain shall call the method `processData()` of the `Personalization` interface if it is implemented by the Applet which is being personalized, otherwise it shall call the method `processData()` of the `Application` interface. The Associated Security Domain is responsible to send this response data out.

The APDU command forwarded by the Security Domain shall be unwrapped according to the Security Level of the current Secure Channel Session. The buffer parameter is the APDU buffer, the offset parameter is set to zero, and the length parameter is set to the length of the unwrapped APDU command message.

The STORE DATA command forwarded to the Applet may be a Case 3 or 4 (ISO/IEC 7816-4[5]) command. The bit 1 (rightmost bit) of the reference control parameter P1 is used to indicate to the card that it is an ISO/IEC 7816-4[5], Case 4 command, and therefore, response data is expected. For a Case 4 command, the Application may or may not return data. For a Case 3 command, response data are not expected and the error code '6A86' is returned if the Applet indicates that response data are available. The Applet may check the Case of the command by looking at the P1 parameter in the APDU buffer.

5.2 `Authority` Interface

This interface provides services to verify a key and to sign data. The CASD shall publish an implementation of this interface to the OPEN as a GlobalService, to make this service available to other Security Domains.

There is only one CASD inside the card. The CASD shall register this service as a unique Global Service with the service family identifier ='83' (per section 8.1.3 of GP221[0]).

6 Tables of Tables

END OF DOCUMENT