GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
Secure Element Protection Profile
Version 1.0

Public Release

February 2021

Document Reference: GPC_SPE_174

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

Figures

Tables

1 Introduction

This document defines the core Protection Profile (PP), functional packages, and PP-Modules for Secure Elements (SEs) implementing Java Card specifications [JCVM], [JCAPI], [JCRE] and GlobalPlatform Card Specification with Amendments [GPCS et al.]. Typical SE form factors include smartcards, eUICCs, and eSEs.

The core PP defines the security problem, objectives, and requirements for SEs by extending the Java Card PP [PP-JC] to address the security functionality defined in [GPCS et al.]. This includes:

- Card and application life cycle management
- Privileges Management
- Trusted Framework
- Secure communication covering all Secure Channel Protocols (SCPs).

The six functional packages defined in chapters 8 to 13 address the following GlobalPlatform privileges assigned to the Security Domains (SDs) or Applications in the card to permit changes to the card content:

- Ciphered Load File Data Block
- Global Services
- Cardholder Verification Method (CVM)
- Delegated Management
- DAP Verification
- Mandated DAP Verification.

GlobalPlatform Amendments B, D, E, F, and G are addressed as part of the core PP. Additionally, four PP-Modules are defined in chapters 14 to 17 to cover Confidential Card Content Management [Amd A], Contactless Services [Amd C], Executable Load File Upgrade [Amd H], and Secure Element Management Service [Amd I]. The Contactless Activation and Contactless Self Activation privileges are covered within the PP-Module for Contactless Services.

A fifth PP-Module defined in chapter 18 addresses the post-issuance OS update capability.

The core PP with its functional packages and the PP-Modules claim conformance to EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5. The SE evaluation may be performed as a composite evaluation [CC-Comp] on top of a certified IC compliant with [PP-0084] or on top of a certified Java Card System compliant with [PP-JC].

The core PP, functional packages, and PP-Modules have been developed by the Security Working Group of the GlobalPlatform SE Committee. They constitute the reference for the evaluation of GlobalPlatform-enabled Java Card SEs.

The allowed SE PP-Configurations consist of the core PP with any of the packages and any subset of PP-Modules.

1.1 Identification

1.1.1 SE PP Identification

Title	Secure Element Protection Profile (SE PP)
Reference	GPC_SPE_174
Date	17 February 2021
Version	1.0
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Mohamad Hajj
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

1.1.2 SE PP-Modules Identification

Title	Confidential Card Content Management (CCCM) PP-Module
Reference	GPC_SPE_194
Date	17 February 2021
Version	1.0
Base PP	SE PP, ref. GPC_SPE_174 version 1.0
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Mohamad Hajj
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	Contactless Services (CTL) PP-Module
Reference	GPC_SPE_195
Date	17 February 2021
Version	1.0
Base PP	SE PP, ref. GPC_SPE_174 version 1.0
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Mohamad Hajj
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	Executable Load File Upgrade (ELFU) PP-Module
Reference	GPC_SPE_196
Date	17 February 2021
Version	1.0
Base PP	SE PP, ref. GPC_SPE_174 version 1.0
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Mohamad Hajj
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	Secure Element Management Services (SEMS) PP-Module
Reference	GPC_SPE_197
Date	17 February 2021
Version	1.0
Base PP	SE PP, ref. GPC_SPE_174 version 1.0
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Mohamad Hajj
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	OS Update PP-Module
Reference	GPC_SPE_198
Date	17 February 2021
Version	1.0
Base PP	SE PP, ref. GPC_SPE_174 version 1.0
Sponsor	GlobalPlatform, Inc.
Author	GlobalPlatform SE Security Working Group
Editor	Mohamad Hajj
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

1.2 Audience

This document is intended primarily for the use of:

- SE Developers: This document presents the set of security requirements to implement.
- SE Issuers and Service Providers: This document allows comparison between products and gives confidence in the product security.
- Evaluators: This document is a normative document for the evaluation.
- Certification Bodies: This document is a normative document for the certification.

1.3 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all of such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any of such IPR.

1.4 References

The tables below list references applicable to this specification. The latest version of each reference applies unless a publication date or version is explicitly stated.

Table 1-1: Normative References

Standard / Specification	Description	Ref
GlobalPlatform Card Specification and Amendments	The following GlobalPlatform Technology specifications: [GPCS] Card Specification [Amd A] Confidential Card Content Management [Amd B] Remote Application Management over HTTP [Amd C] Contactless Services [Amd D] Secure Channel Protocol '03' [Amd E] Security Upgrade for Card Content Management [Amd F] Secure Channel Protocol '11' [Amd G] Opacity Secure Channel [Amd H] Executable Load File Upgrade [Amd I] Secure Element Management Service Each specification is identified in detail below.	[GPCS et al.]
GlobalPlatform Card Specification	GlobalPlatform Technology Card Specification v2.3.1, March 2018 Document Reference: GPC_SPE_034	[GPCS]

Standard / Specification	Description	Ref
GPCS Amendment A	GlobalPlatform Card Confidential Card Content Management Card Specification v2.3 – Amendment A v1.2 or latest applicable version Document Reference: GPC_SPE_007	[Amd A]
GPCS Amendment B	GlobalPlatform Card Remote Application Management over HTTP Card Specification v2.2 – Amendment B v1.1.3 or latest applicable version Document Reference: GPC_SPE_011	[Amd B]
GPCS Amendment C	GlobalPlatform Card Technology Contactless Services Card Specification v2.3 – Amendment C v1.3 or latest applicable version Document Reference: GPC_SPE_025	[Amd C]
GPCS Amendment D	GlobalPlatform Card Technology Secure Channel Protocol '03' Card Specification v2.3 – Amendment D v1.2 or latest applicable version Document Reference: GPC_SPE_014	[Amd D]
GPCS Amendment E	GlobalPlatform Card Technology Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E v1.1 or latest applicable version Document Reference: GPC_SPE_042	[Amd E]
GPCS Amendment F	GlobalPlatform Card Secure Channel Protocol '11' Card Specification v2.3 – Amendment F v1.2.1 or latest applicable version Document Reference: GPC_SPE_093	[Amd F]
GPCS Amendment G	GlobalPlatform Opacity Secure Channel Card Specification v2.3 – Amendment G v1.0 or latest applicable version Document Reference: GPC_SPE_106	[Amd G]
GPCS Amendment H	GlobalPlatform Card Executable Load File Upgrade Card Specification v2.3 – Amendment H v1.1 or latest applicable version Document Reference: GPC_SPE_120	[Amd H]

Standard / Specification	Description	Ref
GPCS Amendment I	GlobalPlatform Technology Secure Element Management Service Card Specification v2.3 – Amendment I v1.0 or latest applicable version Document Reference: GPC_SPE_121	[Amd I]
GlobalPlatform Common Implementation Configuration	GlobalPlatform Card Common Implementation Configuration v2.1 or latest applicable version Document Reference: GPC_GUI_080	[GP CIC]
GlobalPlatform Privacy Framework	GlobalPlatform Card Technology Card Specification – Privacy Framework v1.0.1 or latest applicable version Document Reference: GPC_SPE_100	[GP PF]
GlobalPlatform Cryptographic Algorithm Recommendations	GlobalPlatform Technology Cryptographic Algorithm Recommendations v1.0 or latest applicable version Document Reference: GP_TEN_053	[GP Crypto]
Java Card PP	BSI-CC-PP-0099-V2-2020 – Java Card System - Open Configuration Protection Profile Version 3.1, April 2020	[PP-JC]
CC Part 1	Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1 revision 5	[CC1]
CC Part 2	Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements, April 2017, Version 3.1 revision 5	[CC2]
CC Part 3	Common Criteria for information Technology Security Evaluation, Part 3: Security assurance components, April 2017, Version 3.1 revision 5	[CC3]
CC Composite	Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018	[CC-Comp]
ANSI X9.62:2005	Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)	[ANSI X9.62]
ANSI/INCITS 504-1:2013	INCITS 504-1 – Generic Identity Command Set Part 1: Card Application Command Set	[ANSI 504-1]
ANSSI RGS Annex B1	Annexe B1 au Référentiel général de sécurité (version 2.0) : Choix et dimensionnement des mécanismes cryptographiques	[ANSSI-RGS]
ANSSI-CC-PP 2010/04	(U)SIM Java Card Platform Protection Profile Basic Configuration. ANSSI-CC-PP 2010/04.	[USIM PP]

Standard / Specification	Description	Ref
BSI-CC-PP-0084-2014	Security IC Platform Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014	[PP-0084]
BSI TR-02102-1	BSI Technische Richtlinie TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (Cryptographic Methods: Recommendations and Key Lengths) v2015-01	[TR 02102]
BSI TR-03111, Version 1.11	BSI Technical Guideline TR-03111: Elliptic Curve Cryptography	[TR 03111]
BSI AIS 20 and AIS 31	Evaluation of random number generators Version 0.10 Functionality classes for random number generators, Version 2.0, 18 September 2011	[AIS20], [AIS31]
CEN/EN 419 212	Application Interface for smart cards used as Secure Signature Creation Devices, Part 1 (Basic services) & Part 2 (Additional services), 28/08/2014	[419 212]
ETSI TS 102 225 (Release 6 or higher)	Smart cards; Secured packet structure for UICC based applications, European Telecommunications Standards Institute Technical Committee Smart Card Platform, 2004	[TS 102 225]
ETSI TS 102 226 (Release 6 or higher)	Smart cards; Remote APDU structure for UICC based applications, European Telecommunications Standards Institute Technical Committee Smart Card Platform, 2004	[TS 102 226]
FIPS PUB 140-2	Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules	[FIPS 140-2]
FIPS PUB 180-4	Federal Information Processing Standards Publication 180-4, 2015: Specifications for the Secure Hash Standard: U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology	[FIPS 180-4]
FIPS PUB 186-4	Digital Signature Standard (DSS) FIPS PUB 186-4	[FIPS 186-4]
FIPS 198	National Institute of Standards and Technology (2008) The Keyed-Hash Message Authentication Code (HMAC). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 198-1, July 2008.	[FIPS 198]
Advanced Encryption Standard (AES)	Federal Information Processing Standards Publication 197: Specification for the Advanced Encryption Standard (AES)	[FIPS 197]
ICAO doc 9303	Machine Readable Travel Documents, 7th edition 2015	[ICAO 9303]
ISO/IEC 9797-1	Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher	[ISO 9797-1]

Standard / Specification	Description	Ref
ISO/IEC 10118-3	Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions	[ISO 10118-3]
ISO/IEC 19772/AC1:2014	Information technology – Security techniques – Authenticated encryption [ISO/IEC 19772:2009 with Technical correction]	[ISO 19772]
NIST SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009.	[NIST 800-108]
NIST SP 800-131A	Transitioning the Use of Cryptographic Algorithms and Key Lengths	[NIST 800-131A]
NIST SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001	[NIST 800-38A]
NIST SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005	[NIST 800-38B]
NIST SP 800-56A Revision 2	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Revision 2 May 2013	[NIST 800-56A]
NIST SP 800-56B	Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP) 800-56B, Rev. 2, March 2019	[NIST 800-56B]
NIST SP 800-57 Part 1 revised	Recommendation for Key Management – Part 1: General (Revised) March 2007	[NIST 800-57]
NIST SP 800-67	Barker EB, Mouha N (2017) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP) 800-67, Rev. 2, November 2017.	[NIST 800-67]
NIST SP 800-73-4	Interfaces for Personal Identity Verification – May 2015	[NIST 800-73-4]
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]
RFC 2616	Hypertext Transfer Protocol – HTTP/1.1	[HTTP]
RFC 2818	HTTP over TLS	[HTTPS]
RFC 4279	Pre-Shared Key Cipher Suites for Transport Layer Security (TLS)	[PSK TLS]
RFC 5246	The TLS Protocol – Version 1.2	[TLS 1.2]
RFC 5639	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation	[RFC 5639]

Standard / Specification	Description	Ref
RFC 5758	Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA	[RFC 5758]
PKCS #1	PKCS #1 v2.2: RSA Cryptography Specifications, November 2016	[PKCS#1]
SOG-IS ACM	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms	[SOG-IS_ACM]

Table 1-2: Informative References

Standard / Specification	Description	Ref
Java Card API	Application Programming Interface, Java Card™ Platform, versions 2.2 through 3.1	[JCAPI]
Java Card VM	Virtual Machine Specification, Java Card™ Platform, versions 2.2 through 3.1	[JCVM]
Java Card JCRE	Runtime Environment Specification, Java Card™ Platform, versions 2.2 through 3.1	[JCRE]

1.5 Terminology and Definitions

Selected terms used in this document are included in Table 1-3. Additional terms are defined in [GPCS].

Table 1-3: Terminology and Definitions

Term	Definition
Application	Instance of an Executable Module after it has been installed.
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 (AP)	Entity that owns an application and is responsible for the application's behaviour.
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.
Asymmetric Cryptography	A cryptographic technique that generates and applies a key pair consisting of a public and a private key belonging together. However, it is not practical to compute from the public key the private key which is kept as secret.
Basic Logical Channel	The permanently available interface between the card and an external entity. The Basic Logical Channel is numbered zero.

Term	Definition
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 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	An entity independent from the Issuer and Application Providers, responsible for enforcing specific off-card and on-card security policies. Such a Controlling Authority is represented on-card by a Security Domain which provides specific functionalities supporting the Controlling Authority's security policy.
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-authorised Card Content changes performed by an approved Application Provider.
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.

Term	Definition
Executable Load File (ELF)	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 authorisation, authentication, administration, Post-Issuance application code and data downloading, and transactional processing.
Immutable Persistent Memory	Memory that can only be read.
Issuer	Entity that owns the card and is ultimately responsible for the behaviour of the card.
Issuer Security Domain (ISD)	The primary on-card entity providing support for the control, security, and communication requirements of the card administrator (typically the Issuer).
Key	A cryptographic key stored in a Security Domain. The key is uniquely identified per Security Domain by the two parameters Key Version Number and Key Identifier. 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.
Key Identifier (KID)	One of the two parameters identifying a key. In the context of a cryptographic operation or protocol performed by a Security Domain, the absolute or relative value of the Key Identifier determines the exact function of the key. See also the definition of Key Version Number.
Key set	A set of keys used together by a Security Domain to perform some cryptographic operation or protocol (e.g. Secure Channel Protocol). See also *Secure Channel Key Set*.
Key Version Number (KVN)	One of the two parameters identifying a key. This parameter defines the general purpose of a key; i.e. its applicability for some cryptographic operation or protocol. For example, keys involved in the execution of a Secure Channel Protocol share the same Key Version Number. The term 'version number' is only used for historic reasons and should not be interpreted as such in the current version of this specification. See also the definition of Key Identifier.
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.

Term	Definition
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	A cryptographic value provided by the card (if required by the 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.
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.
SE Platform	It is composed of an open Java Card System extended with the implementation of GlobalPlatform Card Specifications.
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 Key Set	A set of keys used together by a Security Domain to perform a Secure Channel Protocol. Keys belonging to such a key set have the same Key Version Number and consecutive Key Identifiers. The number of keys required within a Secure Channel Key Set depends on the Secure Channel Protocol.
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.
Secure Element (SE)	A tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. May exist in any form factor, such as embedded or integrated SE, SIM/UICC, smart card, smart microSD, etc.

Term	Definition
Security Domain	Application having the Security Domain privilege. This on-card entity provides support for the control, security, and communication requirements of an off-card entity such as 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.
Smart Card Platform	It is comprised of the integrated circuit, the IC dedicated software, and the low-level operating system. (As defined in [PP-JC].)
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.
Tamper-resistant secure hardware	Hardware designed to isolate and protect embedded software and data by implementing appropriate security measures. The hardware and embedded software meet the requirements of the latest Security IC Platform Protection Profile [PP-0084] including resistance to physical tampering scenarios described in that Protection Profile.
Token	A cryptographic value provided by an Issuer as proof that a Delegated Management operation has been authorised.
Trust Point	An authority whose public key is trusted by a Security Domain or Off-Card-Entity through an authority-proprietary and appropriate 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	In the context of this document, the UICC as defined by ETSI Project Smart Card Platform in [TS 102 225] and [TS 102 226].
Verification Authority	A Controlling Authority whose responsibility is to enforce control over card contents using the Mandated DAP Verification mechanism.

1.6 Abbreviations and Notations

Table 1-4 defines the abbreviations used within this Protection Profile.

Table 1-4: Abbreviations and Notations

Abbreviation / Notation	Meaning
AES	Advanced Encryption Standard
AID	Application Identifier

Abbreviation / Notation	Meaning
AM	Authorised Management
AP	Application Provider
APDU	Application Protocol Data Unit
APSD	Application Provider Security Domain
C-MAC	MAC appended to an APDU command
CA	Controlling Authority
CASD	Controlling Authority Security Domain
CA-SEMS	SEMS Certification Authority
CBC	Cipher Block Chaining
CCCM	Confidential Card Content Management
CCM	Card Content Management
CL	Contactless
CLF	Ciphered Load File
CLFDB	Ciphered Load File Data Block
CREL	Contactless Registry Event Listener
CRS	Contactless Registry Service
CTL	Contactless Services
CVM	Cardholder Verification Method
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DM	Delegated Management
ECC	Elliptic Curve Cryptography
eIDAS	Electronic Identification, Authentication and Trust Services
ELF	Executable Load File
ELFU	Executable Load File Upgrade
eSE	Embedded Secure Element
eUICC	Embedded UICC
GS	Global Services
IC	Integrated Circuit
ISD	Issuer Security Domain
MAC	Message Authentication Code
ME	Mobile Equipment (e.g. Mobile Phone, Wearable Device)
MNO	Mobile Network Operator

Abbreviation / Notation	Meaning
NA	Not Applicable
NFC	Near Field Communication
OE	Operational Environment
OS	Operating System
OSP	Organisational Security Policy
OTA	Over-The-Air
PKI	Public Key Infrastructure
PP	Protection Profile
R-MAC	MAC appended to an APDU response.
RGK	Randomly Generated Key
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SAR	Security Assurance Requirement
SCMS	Smart Card Management System
SCP	Secure Channel Protocol
SD	Security Domain
SE	Secure Element
SEI	Secure Element Issuer
SEMS	Secure Element Management Services
SFP	Security Function Policy
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
SP	Service Provider
SPD	Security Problem Definition
SSD	Supplementary Security Domain
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
VA	Verification Authority
ZKM	Zero Key Management

1.7 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-5: Revision History

Date	Version	Description
February 2021	1.0	Public Release

2 TOE Overview

This chapter defines the Target of Evaluation (TOE), presents typical TOE architectures, and describes the TOE's main security features, intended usage, and life cycle.

2.1 TOE Type

The TOE type is an open GlobalPlatform SE implementing the GlobalPlatform Card Specification ([GPCS]) and a Java Card runtime environment.

The TOE provides secure application execution and storage, protection of application code and data from unauthorised access and support for cryptographic key management and operations, CVM management, multi-application deployment, and personalisation.

The TOE is composed of the following components:

- The IC and Dedicated Software certified against [PP-0084].
- The Java Card System including the runtime environment (JCRE), virtual machine (JCVM), and API (JCAPI). Native code may complete this layer. This may be certified according to [PP-JC]. The Java Card System is compliant with Java Card specifications versions 2.2.x or 3.x.x Classic Edition, including post-issuance installation facilities of applications verified off-card.
- The GlobalPlatform Framework as a set of components covering the Card Manager (OPEN), the Trusted Framework, the GlobalPlatform APIs, and the ISD. Note that the APSD(s) and CASD(s) are optional.

The TOE user security guidance is part of the TOE.

This PP extends the Java Card PP Open Configuration [PP-JC] with security requirements for the GlobalPlatform Framework of the TOE. Following the approach used in the Java Card PP, the IC and Dedicates Software are covered by security objectives for the environment. In a conformant Security Target (ST), these become TOE objectives.

Remark: If the TOE provides OS Update functionality then the use of OS Update PP-Module is mandatory. This PP-Module does not address the situation where an entire OS would be replaced as supported in the Package 'Loader' from the [PP-0084]. Only the OS update is addressed here, not the OS replacement.

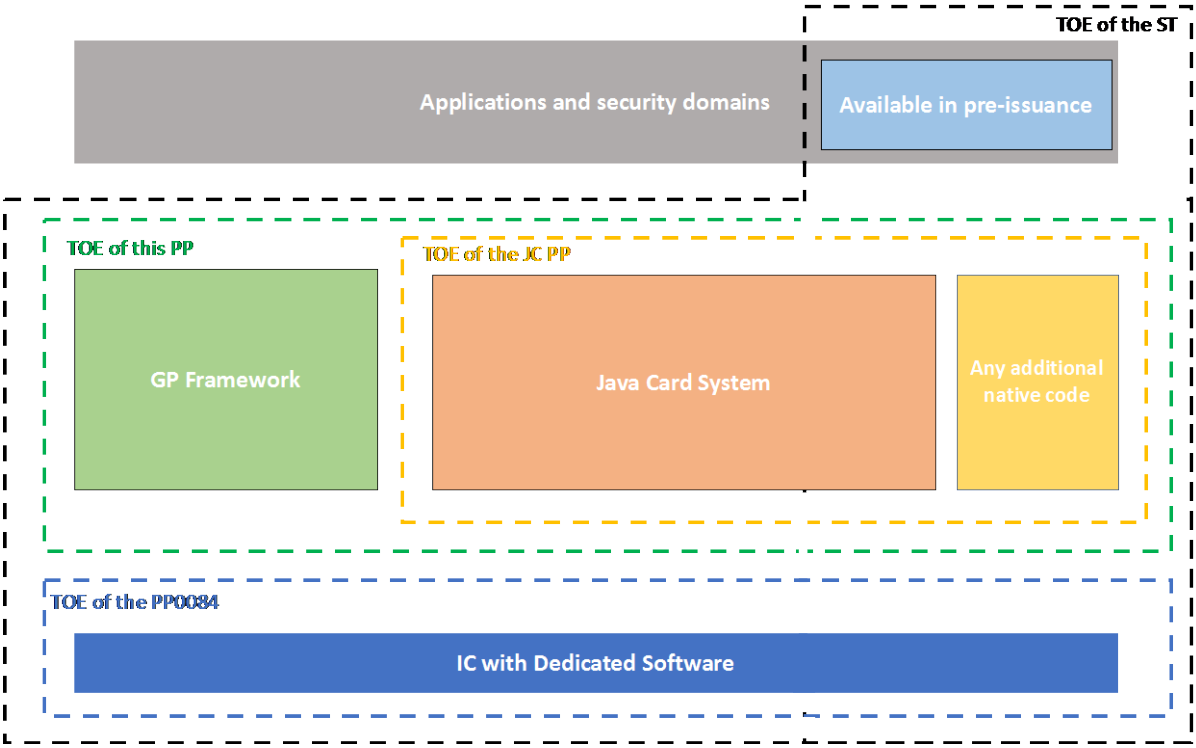
2.2 TOE Description

Figure 2-1 illustrates a logical architecture of the TOE:

- The green dashed line shows the TOE defined in this PP, which includes the GlobalPlatform Framework, the Java Card System and any additional native code. The orange dashed line corresponds to the TOE defined in [PP-JC].
- The scope of an SE evaluation compliant with this PP is represented by the black dashed line. It includes the IC and Dedicated Software and the applications that are known before issuance.
- The blue dashed line shows the IC and Dedicated Software defined in [PP-0084].
- Post-issuance applications and security domains are out of scope of this PP.

The ST author may decide to extend this scope with applicative functionality.

Figure 2-1: TOE Components



2.2.1 GlobalPlatform Functionalities

The GlobalPlatform Framework implements the functionalities described in [GPCS] and possibly some amendments amongst [Amd A], [Amd B], [Amd C], [Amd D], [Amd E], [Amd F], [Amd G], [Amd H], and [Amd I].

The GlobalPlatform functionalities are provided by the following components:

- Security Domains (SDs) as the on-card representatives of off-card authorities. A Security Domain (SD) supports security services such as key handling, encryption, decryption, digital signature generation and verification for the applications of its owner (Issuer, Application Provider, or Controlling Authority). The Issuer Security Domain (ISD) is a mandatory component. An SE that supports multiple SDs can allow an Application Provider, through its own SD, to manage its own Applications and provide cryptographic services using keys that are separate from, and not under the control of, the Issuer.
- GlobalPlatform Environment (OPEN) provides an API to applications, command dispatch, Application selection, (optional) logical channel management, and card content management. 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 privileges defined for Card Content management (DAP Verification, Mandated DAP Verification, Authorised Management, Delegated Management, Token Verification, and receipt generation).
- Secure Channel Protocols SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, and SCP81, provided through the SDs. These protocols support entity authentication, as well as integrity, authenticity, and confidentiality of the payload.

2.2.2 Java Card System Functionalities

The Java Card System implements the functionality described in [JCVM], [JCRE], and [JCAPI]:

- The Java Card Virtual Machine (JCVM) provides the on-card bytecode interpreter.
- The Java Card Runtime Environment (JCRE) is responsible for resource management, isolation between applets, communication, applet execution, and applet security.
- The Java Card Application Programming Interface (JCAPI) provides classes and interfaces for the core functionality. It defines the calling conventions by which an applet can access the JCRE and native services such as, among others, I/O management functions, CVM and cryptographic specific management, and the exceptions mechanism.

The Java Card System is compliant with Java Card specifications versions 2.2.x or 3.x.x Classic Edition, including post-issuance installation facilities of applications verified off-card.

2.3 Major Security Features

The main security features of the SE embedding the TOE consist of the features provided by the underlying IC [PP-0084] and Java Card System [PP-JC] to protect the integrity, confidentiality, and execution of application code and data, plus the features offered by the GlobalPlatform Framework, which are briefly described in this section.

2.3.1 Card and Application Management

The TOE offers security services for card and application management, relying on the GlobalPlatform Framework:

- The Issuer is initially the only entity authorised to manage applications (loading, instantiation, deletion) through a secure communication channel with the card. However, the Issuer can grant this privilege to the Application Provider (AP) through the Delegated Management (DM) or Authorised Management (AM) functionality, if supported by the implementation.
- Loaded applications[1] may be associated at load time to a Verification Authority (VA) signature (Mandated DAP). This signature is verified on card by the on-card-representative of the VA. The verification shall be applied prior to completion of the application loading operation and prior to the instantiation of any applet defined in the loaded application.
- Before loading, application code can be encrypted (Ciphered Load File or CLF) using a key owned by the SD to ensure its confidentiality. The application code will later be decrypted once extradited to the SD of its Application Provider (AP).
- 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 signatures and/or certificates to other off-card entities according to its own security policy.
- Application Providers may personalise their applications and SDs in a confidential manner. Application Providers have SD key sets enabling them to be authenticated to the corresponding SD and to establish a trusted channel between the TOE and an external trusted device. The CA is responsible for securing the creation of SD key sets and the personalisation of the Application Provider Security Domain (APSD) [Amd A]. These key sets are not known by the Issuer.

[1] Note that integrity protection and authorisation are also assumed preconditions by the Java Card PP. This PP assumes that all byte codes are verified at least once before loading, installation, or execution.

- An SD with Receipt Generation privilege is able to generate a receipt acting as a proof of the completion of the requested card content management operations initiated by the SD. This covers the following operations: loading, extradition, installing, removing, and updating the GlobalPlatform Registry operations (see [GPCS]).

2.3.2 Secure Communication Management and Protocols

The TOE provides security services for the mutual authentication with off-card entities and the protection of the information that is exchanged between card and off-card entities. The security level of the communication with an off-card entity does not necessarily apply to each individual message, but the security level depends on the environment and/or the context in which the messages are transmitted. The concept of card life cycle may be used to determine the security level of the communication between the card and an off-card entity. These services are provided through standardised Secure Channel Protocols (SCP) that are available to the applications through their associated SDs (ISD or APSD):

- Entity authentication – in which the card authenticates the off-card entity and the off-card entity may authenticate the card, proving that the off-card entity has knowledge of the same secret(s) as the card;
- Integrity and Data Origin authentication – in which the receiving entity (the card or off-card entity) ensures that the data being received actually came from an authenticated entity (respectively the off-card entity or card) 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 readable by an unauthorised entity.
- Card Content Management (e.g. Applet upload).

All SCPs defined in [GPCS et al.] are covered by the core PP as illustrated in Table 2-1.

This PP does not prescribe the use of one SCP or another. The choice of the SCP and the cryptographic algorithms for securing the communication are specific to the Issuer and Service Providers.

Recommendations for appropriate cryptographic algorithms, key sizes and standards are given in [GP Crypto]. These are aligned with the recommendations issued by NIST [NIST 800-131A], SOG-IS [SOG-IS_ACM], BSI [TR 02102] and ANSSI [ANSSI-RGS].

Table 2-1: GlobalPlatform Secure Channel Protocols

Secure Channel Protocol	Specification	Crypto	Usage
SCP02	[GPCS]	TDES	SCP02 uses Triple DES encryption algorithm in CBC mode with Initialization Vector (IV) of binary zeros. As SCP02 uses TDES in CBC mode with a fixed IV consisting of binary zeros. Therefore, its encryption scheme is deterministic, not highly secure and thus vulnerable to classical plaintext-recovery attacks. For that reason, SCP02 is discontinued in [GPCS] v2.3.1 and the use of an alternative SCP protocol is recommended; e.g. SCP03. **Strong recommendation 1:** • TDES with 2 keys should not be used. Specific care is needed for products already in the market.

Secure Channel Protocol	Specification	Crypto	Usage
			• TDES with 3 keys should not be used for any new products/specifications. Products may already be in the market. • TDES is not considered secured enough. It is advisable to use AES, if one needs long term security.
SCP03	[Amd D]	AES	SCP03 applies the Advanced Encryption Standard (AES) with a randomly generated Initialization Vector (IV). Hence cryptographic analysis of SCP03 is not practical from today's perspective. SCP03 provides protection against replay, out-of-order-delivery and algorithm substitution attacks.
SCP10	[GPCS] and [Amd E]	RSA	SCP10 offers authentication services using an RSA-based Public Key Infrastructure (PKI), secure messaging protection of commands, and responses with the protection of symmetric cryptography. **Strong recommendation 2:** RSA 1024 bit is not considered secured enough. It is advisable to use RSA with 2048 bit or more, if one needs long term security. **Strong recommendation 3:** • The use of PKCS #1 version 1.5 and other RSA key-agreement or key-transport schemes are deprecated. • The use of RSA OAEP is recommended.
SCP11	[Amd F]	ECC	SCP11 offers authentication services using an ECC-based Public Key Infrastructure (PKI), secure messaging protection of commands and responses based on SCP03.
SCP21	[GP PF]	eIDAS	Privacy Framework [GP PF] as recognition of CEN/EN 419 212 [419 212]. Two distinct protocol steps are defined: • PACE (Password Authentication Connection Establishment) • mEAC (modular Extended Access Control) which uses EAC V1 or EAC V2
SCP22	[Amd G]	ECC + Opacity	SCP22 covers the methods of the Opacity Secure Channel establishment including ZKM, FS, and blinded protocols.
SCP80	[TS 102 225] and [TS 102 226]	AES/TDES	SCP80 supports the Over-The-Air security scheme defined in [TS 102 225] and [TS 102 226]. See recommendation 1.
SCP81	[Amd B]	HTTP and PSK TLS	SCP81 supports an Over-The-Air security scheme based on the usage of both HTTP and Pre-Shared Key TLS protocols.

Secure Channel Protocol	Specification	Crypto	Usage
			Strong recommendation 4: The use of TLS version 1.2 is recommended.

2.3.3 Cryptographic Operations

The SE shall support the following types of cryptographic operations:

- Symmetric Encryption/Decryption (TDES, AES)
- Asymmetric Encryption/Decryption (RSA, ECC)
- Signature generation and verification (RSA, ECDSA)
- MACing (R-MAC, C-MAC)
- Random Number Generation
- Key Generation
- Key Derivation (HMAC, CMAC)
- Key Agreement (ECKA-EG)
- Hashing (SHA-256, 384, 512).

The algorithms, key sizes, modes, and applicable standards are given as part of the following security functional requirements:

Table 2-2: Cryptographic Operations

In the core PP	FCS_COP.1/GP-SCP
In Ciphered Load File Data Block package	FCS_COP.1/GP-CLFDB
In Delegated Management package	FCS_COP.1/GP-TOKEN FCS_COP.1/GP-RECEIPT
In DAP Verification package	FCS_COP.1/GP-DAP-SHA FCS_COP.1/GP-DAP-VER
In CCCM PP-Module	FCS_COP.1/GP-CCCM
In SEMS PP-Module	FCS_COP.1/SEMS
In OS Update PP-Module	FCS_COP.1/OS-UPDATE-DEC FCS_COP.1/OS-UPDATE-VER

2.4 TOE Usage

The TOE is used in a variety of scenarios to provide tamper-resistant data and execution protection; for instance:

- Financial applications, such as credit/debit/pre-paid cards
- Transport and ticketing, e.g. granting pre-paid access to a transport system

- Communication, through the Subscriber Identification Module (SIM) or NFC chips or eUICC
- Personal identification/authentication
- Electronic passports and identity cards
- Secure information storage, such as health records or health insurance cards.

2.5 Available Non-TOE Hardware/Software/Firmware

This PP follows the Java Card PP approach, which consists of focusing on the definition of security problems, objectives, and requirements that are specific to Java Card and GlobalPlatform features. Therefore, formally, non-TOE components are the following:

- Bytecode Verifier (off-card component)
- Smart Card Platform, consisting of the IC and Dedicated Software.

As explained in section 2.1, the evaluation of a product against this PP shall include the Smart Card Platform.

2.6 TOE Life Cycle

The overall SE life cycle consists of the following phases (see [PP-0084]):

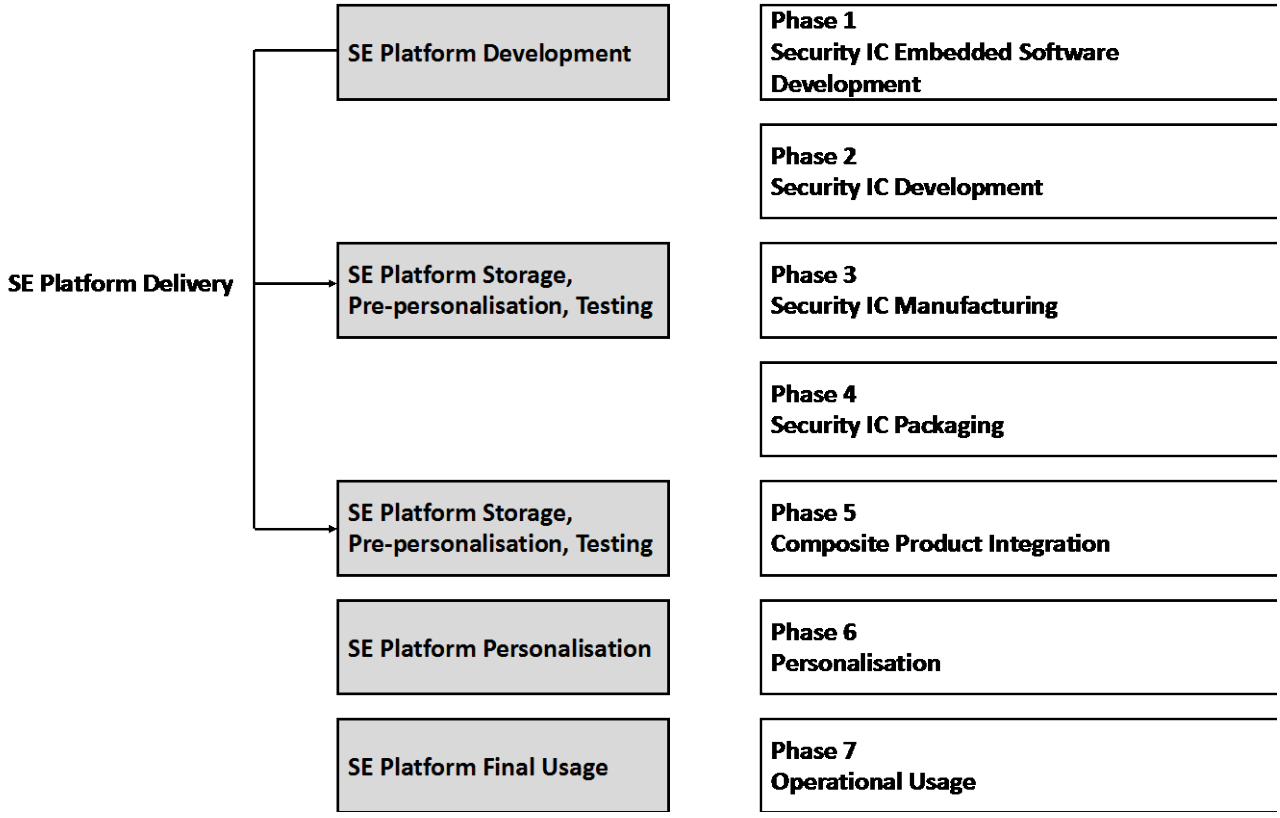
- Phases 1 and 2 compose the product development: IC and Embedded Software (IC Dedicated Software, Java Card System, GlobalPlatform Framework, SDs, Applications) development.
- Phase 3 corresponds to IC manufacturing. Some IC pre-personalisation steps may occur in Phase 3.
- Phase 4 corresponds to IC packaging.
- Phase 5 concerns the embedding of software components within the IC.
- Phase 6 is dedicated to the product personalisation for final use.
- Phase 7 is the product operational phase.

Following [PP-JC], the TOE (software SE platform) life cycle consists of four stages:

- Development
- Storage, pre-personalisation, and testing
- Personalisation and testing
- Final usage.

TOE storage is not necessarily a single step in the life cycle since it can be stored in parts. TOE delivery occurs before storage and may take place more than once if the TOE is delivered in parts. These stages map to the typical smart card life cycle phases as shown in Figure 2-2.

Figure 2-2: TOE (SE Platform) Life Cycle



TOE Development is performed during Phase 1. This includes the Java Card System and the GlobalPlatform Framework conception, design, implementation, testing, and documentation. The TOE development shall fulfil requirements of the final product, including conformance to functional/design specifications (if applicable) and recommendations of the IC user guidance. The TOE development shall be conducted in a controlled and security-protected environment. This environment shall prevent disclosure of source code, data, sensitive and critical documentation, and shall maintain the integrity of these elements. The evaluation of a product against this PP shall include the TOE development environment.

The delivery of the TOE may occur either during the Security IC Manufacturing (Phase 3) or during the Composite Product Integration (Phase 5). It is also possible that a part of the TOE is delivered in Phase 3 and the rest is delivered in Phase 5. Delivery and acceptance procedures shall guarantee the authenticity, confidentiality, and integrity of the exchanged pieces. The TOE delivery shall encrypt and sign the sending presupposing the secure exchange of public keys. The evaluation of a product against this PP shall include the delivery process.

In Phase 3, the Security IC Manufacturer may store, pre-personalise the TOE, and potentially conduct tests on behalf of the developer. The Security IC Manufacturing environment shall protect the integrity and confidentiality of the TOE and of any related material, such as test suites. The evaluation of a product against this PP shall include the whole Security IC Manufacturing environment, particularly those locations where the TOE is accessible for installation or testing. For a Security IC that has already been certified against [PP-0084], there is no need to perform the evaluation again.

In Phase 5, the Composite Product Integrator may store, pre-personalise the TOE, and potentially conduct tests on behalf of the developer. The Composite Product Integration environment shall protect the integrity and confidentiality of the TOE and of any related material, for instance test suites. Note that (part of) the TOE storage in Phase 5 implies a product delivery after Phase 5. Hence, the evaluation of such a product against this PP shall include the Composite Product Integrator environment(s).

The TOE is personalised in Phase 6. The Personalisation environment shall be a controlled environment (secure locations, secure procedures, and trusted personnel). All critical material including personalisation data, test suites, and documentation shall be protected from disclosure and modification. During this phase, ISD keys and other initial data, Certification Authority, Verification Authority, Application Provider(s), and applications data are loaded on the TOE. After this phase, the TOE reaches its INITIALIZED state.

The final SE product with the embedded TOE represents the operational environment of the TOE. It covers a wide spectrum of situations that cannot be covered by evaluations. The TOE and the product shall provide the full set of security functionalities to avoid abuse of the product by untrusted entities.

Card management (including loading of applications and personalisation) can be conducted during the production in a secured area in Phase 5 or 6, or during product usage in Phase 7.

Application Note:

The Security Target writer shall specify the life cycle of the product, the TOE delivery point, and the product delivery point. The product delivery point may arise at the end of Phase 3, 4, or 5. Note that the TOE delivery equals the product delivery as the TOE is an integral part of the product.

2.7 Actors of the TOE

One of the characteristics of the TOE is that several entities are represented inside it:

- **Issuer** (e.g. device manufacturer, MNO, or bank), the owner of the TOE. The TOE guarantees that the Issuer, once authenticated, can manage the loading, instantiation, and deletion of Applications.
- **Application Provider (AP)**, the entity or institution that is responsible for the Applications and their associated services.
- **Controlling Authority (CA)**, the entity, independent from the Issuer, that is responsible for providing on-card security services such as confidential key loading and signature.
- **Verification Authority (VA)**, a Controlling Authority whose responsibility is to enforce control over card content using the Mandated DAP Verification mechanism.

Application Note: See [GPCS] for more information about entities represented within the SE.

2.8 Instructions for ST Authors

The ST shall conform to the core PP and optionally to some functional packages and/or PP-Modules.

The ST author shall indicate the set of selected functional packages and PP-Modules to which the ST claims conformance on top of the core PP.

Table 2-3 presents the privileges that must be associated with the ISD in all implementations, i.e. they are Mandatory (M). It also presents the privileges that are Not Applicable (NA) to some types of entities. X means that a privilege belongs to the core PP.

The ST author shall:

- Indicate if SSDs are supported (YES or NO).
- Complete with YES or NO the “?” cells of the table for all the privileges that are effectively supported by the implementation for the ISD, the SSDs, and the Applications.
- Select the functional packages and PP-Modules indicated in the rightmost columns to cover the implemented privileges. Note that the functional package DAP is mandatory if SSD is supported and that PP-Modules for CCCM [Amd A] and ELFU [Amd H] are not linked to any privilege.

- Select the PP-Modules that are not linked to any privileges, i.e. ELFU, CCCM, and/or OS Update, if the TOE implements the corresponding functionality.

Therefore, the table completed by the ST author shall provide a complete view of the mandatory (M) and optional features effectively implemented by the TOE (YES).

Table 2-3: Functional Packages, PP-Modules, and Privileges Supported by the Implementation

Supported	**M**	**?**	**M**			
Privilege	**ISD**	**SSD**	**Application**	**Core SE PP**	**Package**	**PP-Module**
Security Domain	M	M	NA	X		
Card Lock	M	**?**	**?**	X		
Card Terminate	M	**?**	**?**	X		
Card Reset	**?**	**?**	**?**	X		
Trusted Path	M	**?**	**?**	X		
Global Delete	M	**?**	NA	X		
Global Lock	M	**?**	NA	X		
Global Registry	M	**?**	NA	X		
Final Application	**?**	**?**	**?**	X		
Authorised Management (AM)	M	**?**	NA	X		
CVM Management	**?**	**?**	**?**		CVM	
DAP Verification	**?**	**?**	NA		DAP	
Mandated DAP Verification	**?**	**?**	NA		MDAP	
Delegated Management (DM)	NA	**?**	NA		DM	
Token Verification	M	**?**	NA		DM	
Receipt Generation	M	**?**	NA		DM	
Contactless Activation	**?**	**?**	**?**			CTL
Contactless Self Activation	**?**	**?**	**?**			CTL
Ciphered Load File Data Block (CLFDB)	**?**	**?**	**?**		CLFDB	
Global Service (GS)	**?**	**?**	**?**		GS	
						ELFU
						CCCM
						SEMS
						OS Update

3 Conformance Claims and Consistency Rationale

3.1 CC Conformance Claim

This PP claims conformance to:

- CC Part 2 [CC2] extended with the security functional requirement FCS_RNG.1
- CC Part 3 [CC3].

3.2 Package Claim

This PP claims conformance to EAL4 augmented with:

- ALC_DVS.2 Sufficiency of security measures
- AVA_VAN.5 Advanced methodical vulnerability analysis.

3.3 Conformance Claim of the PP

This PP is conformant to the Java Card System Open Configuration Protection Profile ([PP-JC]).

Application note: Several concepts and definitions given in this PP come from the USIM PP ([USIM PP]) which addresses the card management problem from the MNO's viewpoint. Nevertheless, this PP is generic and does not claim conformance to the USIM PP.

3.4 Conformance Statement

This PP requires demonstrable conformance of any compliant ST or PP.

3.5 Conformance Claim Rationale

The relationship between the core SE PP and the Java Card PP is described hereafter. The relationship between assets, threats, OSPs, assumptions, security objectives, and SFRs uses the following notation:

- Equivalent (E): The element in the core SE PP is the same as in [PP-JC].
- Refinement (R): The element in the core SE PP refines the corresponding [PP-JC] element. New names are given between brackets and added to the list of elements.
- Addition (A): The element is newly defined in the core SE PP; it is not present in [PP-JC] and does not affect it.
- Not Included (NI): The element is defined in [PP-JC] but not included in the core SE PP.
- x: The element is present in [PP-JC].

3.5.1 Conformity of the TOE Type

The TOE type for this PP extends the Java Card System defined in [PP-JC].

3.5.2 SPD Consistency

3.5.2.1 Assets

All assets defined in [PP-JC] are relevant for the TOE of this PP. There are six new assets, three of them originate in an asset defined in [PP-JC].

The table below indicates the assets' consistency statement.

Table 3-1: Assets Consistency Statement

Assets	[PP-JC]	Core SE PP
D.API_DATA	x	E
D.CRYPTO	x	E
D.JCS_CODE	x	E
D.JCS_DATA	x	E
D.SEC_DATA	x	E
D.APP_CODE	x	E
D.APP_C_DATA	x	E
D.APP_I_DATA	x	E
D.APP_KEYS	x	R: D.ISD_KEYS, D.APSD_KEYS, D.CASD_KEYS
D.PIN	x	E
D.ISD_KEYS		A
D.APSD_KEYS		A
D.CASD_KEYS		A
D.TOE_IDENTIFIER		A
D.GP_REGISTRY		A
D.GP_CODE		A

The assets D.APSD_KEYS, D.CASD_KEYS, and D.ISD_KEYS are refinements of the asset D.APP_KEYS in the [PP-JC]. All coexist in this PP.

3.5.2.2 Users and Subjects

All subjects in the [PP-JC] are relevant for the TOE of this PP. There are two additional subjects.

The table below indicates the subjects' consistency statement.

Table 3-2: Subjects Consistency Statement

Subjects	[PP-JC]	Core SE PP
S.ADEL	x	R: S.OPEN
S.APPLET	x	E
S.BCV	x	E
S.CAD	x	E
S.INSTALLER	x	R: S.OPEN
S.JCRE	x	E
S.JCVM	x	E
S.LOCAL	x	E
S.MEMBER	x	E
S.CAP_FILE	x	E
S.SD		A
S.OPEN		A

The subjects S.ADEL and S.INSTALLER defined in the [PP-JC] are covered by S.OPEN in this PP.

3.5.2.3 Threats

All threats in the [PP-JC] are relevant for the TOE in this PP. There are four new threats.

The table below contains the threats' consistency statement.

Table 3-3: Threats Consistency Statement

Threats	[PP-JC]	Core SE PP
T.CONFID-APPLI-DATA	x	E
T.CONFID-JCS-CODE	x	E
T.CONFID-JCS-DATA	x	E
T.INTEG-APPLI-CODE	x	E
T.INTEG-APPLI-CODE.LOAD	x	E
T.INTEG-APPLI-DATA	x	E
T.INTEG-APPLI-DATA.LOAD	x	E
T.INTEG-JCS-CODE	x	E
T.INTEG-JCS-DATA	x	E
T.SID.1	x	E
T.SID.2	x	E
T.EXE-CODE.1	x	E
T.EXE-CODE.2	x	E

Threats	[PP-JC]	Core SE PP
T.NATIVE	x	E
T.RESOURCES	x	E
T.DELETION	x	R: T.UNAUTHORISED-CARD-MGMT
T.INSTALL	x	R: T.UNAUTHORISED-CARD-MGMT
T.OBJ-DELETION	x	E
T.PHYSICAL	x	E
T.COM-EXPLOIT		A
T.UNAUTHORISED-CARD-MGMT		A
T.LIFE-CYCLE		A
T.BRUTE-FORCE-SCP		A

The threats T.INSTALL and T.DELETION defined in the [PP-JC] are covered by T.UNAUTHORISED-CARD-MGMT in this PP.

T.COM-EXPLOIT is included to cover communication channels attacks.

T.LIFE-CYCLE is included to cover content management attacks.

T.BRUTE-FORCE-SCP is included to cover brute force attacks.

3.5.2.4 Organisational Security Policy (OSP)

The OSP.VERIFICATION defined in the [PP-JC] is relevant for the TOE of this PP. Ten new OSPs are introduced.

The table below provides the OSPs' consistency statement.

Table 3-4: OSP Consistency Statement

OSPs	[PP-JC]	Core SE PP
OSP.VERIFICATION	x	E
OSP.AID-MANAGEMENT		A
OSP.LOADING		A
OSP.SERVERS		A
OSP.APSD-KEYS		A
OSP.KEY-GENERATION		A
OSP.CASD-KEYS		A
OSP.KEY-CHANGE		A
OSP.SECURITY-DOMAINS		A
OSP.ISD-KEYS		A
OSP.APPLICATIONS		A

3.5.2.5 Assumptions

All the assumptions defined in the [PP-JC] are relevant for the TOE in this PP except A.DELETION which is excluded as the card manager belongs to the TOE. There are ten additional assumptions in this PP.

The table below provides the assumptions' consistency statement.

Table 3-5: Assumptions Consistency Statement

Assumptions	[PP-JC]	Core SE PP
A.CAP_FILE	x	E
A.DELETION	x	Excluded
A.VERIFICATION	x	E
A.ADMIN		A
A.APPS-PROVIDER		A
A.VERIFICATION-AUTHORITY		A
A.KEY-ESCROW		A
A.PERSONALISER		A
A.CONTROLLING-AUTHORITY		A
A.PRODUCTION		A
A.ISSUER		A
A.SCP-SUPP		A
A.KEYS-PROT		A

A.DELETION is excluded because O.DELETION is an objective for the TOE.

3.5.3 Security Objectives Consistency Statement

3.5.3.1 Security Objectives for the TOE

All the security objectives for the TOE defined in the [PP-JC] are relevant for this TOE in this PP. These have been completed with ten additional objectives.

The table below provides the consistency statement for the 'security objectives for the TOE'.

Table 3-6: 'Security Objectives for the TOE' Consistency Statement

Objectives for the TOE	[PP-JC]	Core SE PP
O.SID	x	E
O.FIREWALL	x	E
O.GLOBAL_ARRAYS_CONFID	x	E
O.GLOBAL_ARRAYS_INTEG	x	E
O.ARRAY_VIEWS_CONFID	x	E

Objectives for the TOE	[PP-JC]	Core SE PP
O. ARRAY_VIEWS_INTEG	x	E
O.NATIVE	x	E
O.OPERATE	x	E
O.REALLOCATION	x	E
O.RESOURCES	x	E
O.ALARM	x	E
O.CIPHER	x	E
O.RNG	x	E
O.KEY-MNGT	x	E
O.PIN-MNGT	x	E
O.TRANSACTION	x	E
O.OBJ-DELETION	x	E
O.DELETION	x	E
O.LOAD	x	E
O.INSTALL	x	E
O.CARD-MANAGEMENT		A
O.DOMAIN-RIGHTS		A
O.APPLI-AUTH		A
O.COMM-AUTH		A
O.COMM-INTEGRITY		A
O.COMM-CONFIDENTIALITY		A
O.SECURITY-DOMAINS		A
O.NO-KEY-REUSE		A
O.PRIVILEGES-MANAGEMENT		A
O.LC-MANAGEMENT		A

3.5.3.2 Security Objectives for the Operational Environment

All the security objectives for the TOE operational environment defined in the [PP-JC] except OE.CARD-MANAGEMENT are relevant for this TOE in this PP. These have been completed with twenty additional objectives for the environment.

The table below provides the consistency statement of the ‘security objectives for the operational environment’.

Table 3-7: 'Security Objectives for the Operational Environment' Consistency Statement

Objectives for the Environment	[PP-JC]	Core SE PP
OE.CAP_FILE	x	E
OE.CARD-MANAGEMENT	x	Removed and replaced by O.CARD-MANAGEMENT
OE.SCP.IC	x	E
OE.SCP.RECOVERY	x	E
OE.SCP.SUPPORT	x	E
OE.VERIFICATION	x	E
OE.CODE-EVIDENCE	x	E
OE.ADMIN		A
OE.APPS-PROVIDER		A
OE.VERIFICATION-AUTHORITY		A
OE.KEY-ESCROW		A
OE.PERSONALISER		A
OE.CONTROLLING-AUTHORITY		A
OE.SCP-SUPP		A
OE.KEYS-PROT		A
OE.PRODUCTION		A
OE.AID-MANAGEMENT		A
OE.LOADING		A
OE.SERVERS		A
OE.AP-KEYS		A
OE.KEY-GENERATION		A
OE.CA-KEYS		A
OE.VA-KEYS		A
OE.KEY-CHANGE		A
OE.ISSUER		A
OE.ISD-KEYS		A
OE.APPLICATIONS		A

OE.CARD-MANAGEMENT defined in [PP-JC] becomes an objective for the TOE as the card manager belongs to the TOE in this PP.

3.5.4 Consistency Statements

3.5.4.1 Consistency of Policies

All the security policies defined in the [PP-JC] are relevant for the TOE of this PP as shown in the table below.

Table 3-8: Policies Consistency Statement

[PP-JC]	Core SE PP	Changes
Package Loading information flow control SFP	ELF Loading information flow control SFP	The term “Package” is replaced by “ELF” as stated in [GPCS].
--	Data & Key Loading information flow control SFP	Addition for loading of the SD/Application keys and data through STORE DATA and PUT KEY commands.

3.5.4.2 Consistency of SFRs

All the SFRs defined in the [PP-JC] are relevant for the TOE in this PP. Twenty-seven SFRs have been refined and seventeen have been added.

All the operations performed on the Java Card SFRs are appropriate for the TOE, which includes the full Java Card System.

Table 3-9: SFRs Consistency Statement

SFRs	[PP-JC]	Core SE PP
FDP_ACC.2/FIREWALL	x	E
FDP_ACF.1/FIREWALL	x	E
FDP_IFC.1/JCVM	x	E
FDP_IFF.1/JCVM	x	E
FDP_RIP.1/OBJECTS	x	E
FMT_MSA.1/JCRE	x	E
FMT_MSA.1/JCVM	x	E
FMT_MSA.2/FIREWALL_JCVM	x	E
FMT_MSA.3/FIREWALL	x	E
FMT_MSA.3/JCVM	x	E
FMT_SMF.1	x	E
FMT_SMR.1	x	E
FCS_CKM.1	x	E
FCS_CKM.4	x	E
FCS_COP.1	x	E
FCS_RNG.1	x	E

SFRs	[PP-JC]	Core SE PP
FDP_RIP.1/ABORT	x	E
FDP_RIP.1/APDU	x	E
FDP_RIP.1/bArray	x	E
FDP_RIP.1/GlobalArray	x	E
FDP_RIP.1/KEYS	x	E
FDP_RIP.1/TRANSIENT	x	E
FDP_ROL.1/FIREWALL	x	E
FAU_ARP.1	x	E
FDP_SDI.2/DATA	x	E
FPR_UNO.1	x	E
FPT_FLS.1	x	E
FPT_TDC.1	x	E
FIA_ATD.1/AID	x	E
FIA_UID.2/AID	x	E
FIA_USB.1/AID	x	E
FMT_MTD.1/JCRE	x	E
FMT_MTD.3/JCRE	x	E
FDP_ITC.2/Installer	x	R: FDP_ITC.2/GP-ELF (Editorial Refinement)
FMT_SMR.1/Installer	x	R: FMT_SMR.1/GP (Editorial Refinement)
FPT_FLS.1/Installer	x	R: FPT_FLS.1/GP (Editorial Refinement)
FPT_RCV.3/Installer	x	R: FPT_RCV.3/GP (Editorial Refinement)
FDP_ACC.2/ADEL	x	E
FDP_ACF.1/ADEL	x	E
FDP_RIP.1/ADEL	x	E
FMT_MSA.1/ADEL	x	E
FMT_MSA.3/ADEL	x	E
FMT_SMF.1/ADEL	x	E
FMT_SMR.1/ADEL	x	E
FPT_FLS.1/ADEL	x	E
FDP_RIP.1/ODEL	x	E
FPT_FLS.1/ODEL	x	E
FCO_NRO.2/CM	x	R: FCO_NRO.2/GP (Editorial Refinement)
FDP_IFC.2/CM	x	R: FDP_IFC.2/GP-ELF (Editorial Refinement)

SFRs	[PP-JC]	Core SE PP
FDP_IFF.1/CM	x	R: FDP_IFF.1/GP-ELF (Editorial Refinement)
FDP_UIT.1/CM	x	R: FDP_UIT.1/GP (Editorial Refinement)
FIA_UID.1/CM	x	R: FIA_UID.1/GP (Editorial Refinement)
FMT_MSA.1/CM	x	R: FMT_MSA.1/GP (Editorial Refinement)
FMT_MSA.3/CM	x	R: FMT_MSA.3/GP (Editorial Refinement)
FMT_SMF.1/CM	x	R: FMT_SMF.1/GP (Editorial Refinement)
FMT_SMR.1/CM	x	R: FMT_SMR.1/GP (Editorial Refinement)
FTP_ITC.1/CM	x	R: FTP_ITC.1/GP (Editorial Refinement)
FDP_UCT.1/GP		A
FPT_TDC.1/GP		A
FDP_ROL.1/GP		A
FPR_UNO.1/GP		A
FIA_UAU.1/GP		A
FIA_UAU.4/GP		A
FIA_AFL.1/GP		A
FMT_MTD.3/GP		A
FMT_SMR.1/GP		R: Refinement of FMT_SMR.1/Installer and FMT_SMR.1/CM
FPT_FLS.1/GP		R: Refinement of FPT_FLS.1/Installer
FPT_RCV.3/GP		R: Refinement of FPT_RCV.3/Installer
FCO_NRO.2/GP		R: Refinement of FCO_NRO.2/CM
FDP_UIT.1/GP		R: Refinement of FDP_UIT.1/CM
FIA_UID.1/GP		R: Refinement of FIA_UID.1/CM
FMT_SMF.1/GP		R: Refinement of FMT_SMF.1/CM
FTP_ITC.1/GP		R: Refinement of FTP_ITC.1/CM
FMT_MSA.1/GP		R: Refinement of FMT_MSA.1/CM
FMT_MSA.3/GP		R: Refinement of FMT_MSA.3/CM
FMT_MTD.1/GP-PR		A
FDP_ITC.2/GP-ELF		R: Refinement of FDP_ITC.2/Installer
FDP_IFC.2/GP-ELF		R: Refinement of FDP_IFC.2/CM
FDP_IFF.1/GP-ELF		R: Refinement of FDP_IFF.1/CM
FDP_ITC.2/GP-KL		A
FDP_IFC.2/GP-KL		A
FDP_IFF.1/GP-KL		A

SFRs	[PP-JC]	Core SE PP
FMT_MTD.1/GP-LC		A
FTP_TRP.1/GP-TF		A
FCS_RNG.1/GP-SCP		A
FCS_CKM.1/GP-SCP		A
FCS_COP.1/GP-SCP		A

3.5.4.3 Consistency of SARs

This PP claims the same evaluation assurance level as [PP-JC], i.e. EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

3.5.5 Consistency of PP-Modules and Packages

All Assets, Users, SPDs, Objectives, and SFRs from [PP-JC] are relevant when the PP-Modules and Packages defined in this PP are used.

4 Security Problem Definition

This chapter introduces the security problem addressed by the TOE and its operational environment. The security problem consists of the threats the SE Platform may face in the field, the assumptions on its operational environment, and the organisational policies that have to be implemented by the SE or within the operational environment.

4.1 Assets

The assets to be protected by the TOE are listed below. They are grouped according to whether it is data created by and for the user (User data) or data created by and for the TOE (TSF data).

The definition of the assets from [PP-JC] is not repeated here.

4.1.1 User Data

Table 4-1: Additional User Data Assets Related to [GPCS]

D.ISD_KEYS	Refinement of D.APP_KEYS of [PP-JC]. ISD cryptographic keys needed to perform card management operations on the card. To be protected from unauthorised disclosure and modification.
D.APSD_KEYS	Refinement of D.APP_KEYS of [PP-JC]. APSD cryptographic keys needed to establish Secure Channels with the AP. These keys can be used to load and install applications on the card if the Security Domain has the appropriate privileges. To be protected from unauthorised disclosure and modification.
D.CASD_KEYS	Refinement of D.APP_KEYS of [PP-JC]. CASD cryptographic keys needed to establish Secure Channels with the CA and to decrypt confidential content for APSDs. To be protected from unauthorised disclosure and modification.

4.1.2 TSF Data

Table 4-2: Additional TSF Data Assets Related to [GPCS]

D.GP_REGISTRY	The information resource for Card Content management. The GlobalPlatform Registry contains information for managing the card, as well as Executable Load Files, Applications, SD associations, privileges, Identifiers, life cycle states, and memory resource quotas. To be protected from unauthorised modification.
D.GP_CODE	The code of the GlobalPlatform Framework on the card. To be protected from unauthorised modification.
D.TOE_IDENTIFIER	TOE Identification Data to identify the TOE.

4.2 Users / Subjects

The definition of subjects from [PP-JC] is not repeated here.

Table 4-3: Additional Subjects Related to [GPCS]

S.SD	A GlobalPlatform SD representing an off-card entity on the card. This entity can be the Issuer, an Application Provider, the Controlling Authority, or the Validation Authority.
S.OPEN	It represents the GlobalPlatform Environment (OPEN) on the card. The main responsibility of the S.OPEN is to provide an API to applications, command dispatch, Application selection, (optional) logical channel management, Card Content management, memory management, and Life Cycle management. S.ADEL and S.INSTALLER are parts of S.OPEN.

4.3 Threats

This section introduces the threats to the assets against which specific protection within the TOE or its environment is required.

The core PP adds specific threats related to Card Management and Secure Communication, as defined in [GPCS].

4.3.1 Java Card System

The definition of threats from [PP-JC] is not repeated here.

4.3.2 Card Management

Table 4-4: Additional Threats for Card Management

T.UNAUTHORISED-CARD-MGMT	Threat agent: Attacker Adverse action: The attacker performs unauthorised card management operations (for instance impersonates one of the actors represented on the card) in order to take benefit of the privileges or services granted to this actor on the card and perform fraudulent operations: • Load of a package file • Installation of a package file • Extradition of a package file or an applet • Personalisation of an applet or an SD • Deletion of a package file or an applet • Privileges update of an applet or an SD Directly threatened asset(s): D.ISD_KEYS, D.APSD_KEYS, D.APP_C_DATA, D.APP_I_DATA, D.APP_CODE, D.SEC_DATA, D.PIN, and D.GP_REGISTRY (any other asset may be jeopardised should this attack succeed, depending on the virulence of the installed application).
T.LIFE-CYCLE	Threat agent: Attacker Adverse action: An attacker accesses an application outside of its expected availability range thus violating irreversible life cycle phases of the application (for instance, an attacker re-personalises the application). Directly threatened asset(s): D.APP_I_DATA, D.APP_C_DATA, and D.GP_REGISTRY.

4.3.3 Secure Communication

Table 4-5: Additional Threats for Secure Communication

T.COM-EXPLOIT	Threat agent: Attacker Adverse action: An attacker remotely exploits the communication channels established between a third party and the TOE in order to modify or disclose confidential data. Directly threatened asset(s): All assets are threatened.
T.BRUTE-FORCE-SCP	Threat agent: Attacker Adverse action: APDU commands/API methods can be repeatedly transmitted/invoked to search the entire space of secret values such as cryptographic keys and attempt their brute force extraction. Directly threatened asset(s): All assets are threatened.

4.4 Organisational Security Policies (OSP)

This section presents the organisational security policies to be enforced with respect to the TOE environment.

The definition of OSPs from [PP-JC] is not repeated here.

Table 4-6: Additional OSPs Related to [GPCS]

OSP.AID-MANAGEMENT	When loading an application that uses shareable object interface, to make its services available to other applications, the VA shall verify that the AID of the application being loaded does not impersonate the AID known by another application on the card for the use of shareable services.
OSP.LOADING	Application code, validated or certified depending on the application, is loaded onto the SE Platform using any kind of CCM servers (e.g. OTA or other kinds of servers used to perform card content management) and protocols with contactless or contact (e.g. USB) connectivity. If needed, the Issuer can pre-authorise content loading operation through delegated management privilege to an individual on-card representative of APs. In that case the application code is loaded in the APSD. Once loaded, the application is personalised using the appropriate SD keys.
OSP.SERVERS	A security policy shall be employed by the Issuer to ensure the security of the applications stored on its CCM servers (e.g. OTA or other kinds of servers used to perform card content management).
OSP.APSD-KEYS	The APSD keys personalisation can rely either on the key escrow if the APSD has been created before the usage phase of the SE card, or on the CA if the APSD has been created during the usage phase. In the first case, the APSD keys are generated and stored in a secure way by the personaliser. Then, these keys are transmitted to the AP, via the key escrow. In the second case, one of the following must occur: • The APSD keys are generated and stored in a secure way by the APSD, then securely transmitted to the AP using the CASD. • Or the APSD keys are created by the AP and securely transferred to the APSD using the CASD.
OSP.ISD-KEYS	The security of the ISD keys shall be ensured by a well-defined security policy that covers generation, storage, distribution, destruction, and recovery. This policy is enforced by the Issuer in collaboration with the personaliser.
OSP.KEY-GENERATION	The personaliser shall enforce a policy ensuring that generated keys cannot be accessed in plaintext.
OSP.CASD-KEYS	The CASD keys shall be securely generated and stored in the SE card during the personalisation process. These keys are not modifiable after card issuance.
OSP.KEY-CHANGE	The AP shall change its initial keys before any operation on its APSD.
OSP.SECURITY-DOMAINS	SDs can be dynamically created, deleted, and blocked during usage phase, i.e. post-issuance.
OSP.APPLICATIONS	The applications intending to be used with the TOE shall follow the TOE's security guidance and recommendations.

4.5 Assumptions

This section states the assumptions that hold on the SE operational environment.

The definition of the assumptions from [PP-JC] is not repeated here.

Table 4-7: Additional Assumptions Related to [GPCS]

A.ISSUER	This is the entity that owns the SE and is ultimately responsible for the behaviour of the SE.
A.ADMIN	These administrators of the CCM servers (e.g. OTA or other kinds of servers) used to perform card content management are trusted actors. They are trained to use and administrate those servers securely. They have the means and the equipment to perform their tasks. They are aware of the sensitivity of the assets they manage and the responsibilities associated with the administration of CCM servers. Administrators obey the security policies and constitute, by this assumption, no source of an inside attack.
A.APPS-PROVIDER	The AP is a trusted actor that provides applications. APs are responsible for their APSD keys.
A.VERIFICATION-AUTHORITY	The VA is a trusted actor with the capability to check and validate the digital signature of an application.
A.KEY-ESCROW	The key escrow is a trusted actor in charge of the secure storage of the initial APSD keys generated by the TOE personaliser during the initial personalisation.
A.PERSONALISER	The personaliser is in charge of the TOE personalisation process, which ensures the security of the keys loaded in the SE: • Issuer Security Domain keys (ISD keys) • Application Provider Security Domains keys (APSD keys) • Controlling Authority Security Domain keys (CASD keys)
A.CONTROLLING-AUTHORITY	The CA is a trusted actor different from the issuer responsible for the CASD keys and associated services.
A.PRODUCTION	Security procedures are used after TOE Delivery up to delivery to the end consumer to maintain the confidentiality and integrity of the TOE and its data (to prevent any possible copy, modification, retention, theft, or unauthorised use).
A.SCP-SUPP	The operational environment supports and uses the SCPs offered by the TOE.
A.KEYS-PROT	The keys stored outside the TOE and applied for secure communication and authentication between the SE and the external entities are confidentiality and integrity protected in their storage environment. This covers D.APSD_KEYS and D.ISD_KEYS.

5 Security Objectives

5.1 Security Objectives for the TOE

This section introduces the security objectives for the TOE.

5.1.1 Java Card System

The definition of the security objectives for the TOE from [PP-JC] is not repeated here.

5.1.2 Card Management

Table 5-1: Additional Objectives for Card Management

O.CARD-MANAGEMENT	The TOE shall provide the card manager as defined in [GPCS]. The card manager shall control the access to card management functions such as the installation, update, or deletion of applets. It shall also implement the Issuer's policy on the card. The card manager is an application with specific rights (e.g. ISD), which is responsible for the administration of the SE. Typically, the card manager shall be in charge of the life cycle of the whole card, as well as that of the installed applications (applets). The card manager shall prevent card content management operations (loading, installation, deletion) from being carried out, for instance, at invalid states of the card or by unauthorised actors. It shall also enforce security policies established by the Issuer.
O.DOMAIN-RIGHTS	The Issuer shall not access or change personalised APSD keys, which belong exclusively to the AP. Modification of an SD key set is restricted to the AP owning the SD.
O.APPLI-AUTH	The card manager shall enforce the application security policies established by the Issuer. The enforcement shall be implemented by requiring application authentication during application loading on the card.
O.SECURITY-DOMAINS	SDs can be dynamically created, deleted, and blocked during the end use phase.

5.1.3 Secure Communication

Table 5-2: Additional Objectives of Secure Communication

O.COMM-AUTH	The TOE shall authenticate the origin of the card management requests received by the card, and authenticate itself to the remote actor.
O.COMM-INTEGRITY	The TOE shall verify the integrity of the (card management) requests that the card receives.
O.COMM-CONFIDENTIALITY	The TOE shall be able to process card management requests containing encrypted data.
O.NO-KEY-REUSE	The TOE shall ensure that session keys can be used only once.

5.1.4 Privileges and Life Cycle Management

Table 5-3: Additional Objectives of Privileges and Life Cycle Management

O.PRIVILEGES-MANAGEMENT	The TOE shall provide Privileges assignment and management functionalities for the on-card entities ISD, SSD, and Applications. The TOE shall control the access to the Privileges assignment and management functions.
O.LC-MANAGEMENT	The TOE shall provide a state machine that enforces the TOE's life cycle, keeps track of the TOE's current state, and controls that the operations required by the users are consistent with the current life cycle state of the TOE. The TOE shall provide Life Cycle (LC) management functionalities for the Card, ELFs, SDs, and Applications.

5.2 Security Objectives for the Operational Environment

This section introduces the security objectives to be achieved by the environment.

5.2.1 Java Card System

The definition of security objectives for the environment from [PP-JC] is not repeated here.

5.2.2 Actors

Table 5-4: Additional OEs for Actors

OE.ISSUER	The Issuer shall be a trusted actor responsible for the behaviour of the SE.
OE.ADMIN	The administrators of the CCM servers (e.g. OTA or other kinds of servers) shall be trusted actors. They shall be trained to use and administrate those servers. They have the means and the equipment to perform their tasks. They must be aware of the sensitivity of the assets they manage and the responsibilities associated with the administration of CCM servers. Administrators obey the security policies and constitute, by this OE, no source of an inside attack.
OE.APPS-PROVIDER	The AP shall be a trusted actor that provides applications. The AP must be responsible for the APSD keys.
OE.VERIFICATION-AUTHORITY	The VA shall be a trusted actor with the capability to check and validate the digital signature attached to an application.
OE.KEY-ESCROW	The key escrow shall be a trusted actor in charge of the secure storage of the AP initial keys generated by the personaliser.

OE.PERSONALISER	The personaliser shall be a trusted actor in charge of the personalisation process. The personaliser shall ensure the security of the keys managed and loaded into the card: • Issuer Security Domain keys (ISD keys), • Application Provider Security Domain keys (APSD keys), • Controlling Authority Security Domain keys (CASD keys).
OE.CONTROLLING-AUTHORITY	The CA shall be a trusted actor responsible for securing the creation and personalisation of APSD keys. The CA must be responsible for the CASD keys.
OE.SCP-SUPP	Secure Communication Protocols shall be supported and used by the operational environment.
OE.KEYS-PROT	During the TOE's use, the terminal in interaction with the TOE shall ensure the protection (integrity and confidentiality) of the applied keys by operational means and/or procedures.

5.2.3 Secure Places

Table 5-5: Additional OEs for Secure Places

OE.PRODUCTION	Security procedures shall be used after TOE Delivery up to delivery to the end consumer to maintain confidentiality and integrity of the TOE and of its data (to prevent any possible copy, modification, retention, theft, or unauthorised use).

5.2.4 Validation

Table 5-6: Additional OEs for Validation

OE.APPLICATIONS	Developers and Validators shall comply with the security guidance and ensure that the rules are enforced.
OE.AID-MANAGEMENT	The VA shall verify that the AID of the application being loaded does not impersonate the AID known by another application on the card for the use of shareable services.

5.2.5 Loading

Table 5-7: Additional OEs for Loading

OE.LOADING	Application code, validated or certified depending on the application, is loaded onto the SE Platform using any kind of CCM servers (e.g. OTA or other kinds of servers used to perform card content management) and protocols with contactless or contact (e.g. USB) connectivity.
OE.SERVERS	The Issuer must enforce a policy to ensure the security of the applications stored on its CCM servers (e.g. OTA or other kinds of servers used to perform card content management).

5.2.6 Keys

Table 5-8: Additional OEs for Keys

OE.AP-KEYS	The SD-key-personaliser, the AP, and the key escrow must enforce a security policy securing the transmissions.
OE.ISD-KEYS	The security of the ISD keys must be ensured in the environment of the TOE.
OE.KEY-GENERATION	The personaliser must ensure that the generated keys cannot be accessed by unauthorised users.
OE.CA-KEYS	The CASD keys must be securely generated prior to storage in the SE card.
OE.KEY-CHANGE	The AP must change the initial keys of APSD before any operation on it.

5.3 Security Objectives Rationale

5.3.1 Threats

T.COM-EXPLOIT This threat is covered by the following security objectives:

- O.COMM-AUTH prevents unauthorised users from initiating a malicious card management operation.
- O.COMM-INTEGRITY protects the integrity of the card management data while it is in transit to the card.
- O.COMM-CONFIDENTIALITY prevents disclosure of encrypted data transiting to the card.

T.UNAUTHORISED-CARD-MGMT This threat is covered by the following security objectives:

- O.CARD-MANAGEMENT controls the access to card management functions such as the loading, installation, extradition, or deletion of applets.
- O.COMM-AUTH prevents unauthorised users from initiating a malicious card management operation.
- O.COMM-INTEGRITY protects the integrity of the card management data while it is in transit to the card.
- O.COMM-CONFIDENTIALITY prevents disclosure of encrypted data transiting to the card.
- O.APPLI-AUTH requires that each application be authenticated before loading.
- O.DOMAIN-RIGHTS restricts the modification of an AP security domain key set to the AP owning it.
- O.PRIVILEGES-MANAGEMENT enforces the Privileges assignment and management functionalities for the on-card entities ISD, SSD, and Applications.
- O.LC-MANAGEMENT enforces the Life Cycle management for the Card, ELFs, SDs, and Applications.

T.LIFE-CYCLE This threat is covered by the security objectives:

- O.CARD-MANAGEMENT controls the access to the card management functions of loading, installation, extradition, and deletion of applets. Attacks for modification or exploitation of the current life cycle of applications are thus rendered impractical.
- O.DOMAIN-RIGHTS restricts the use of an AP security domain key set and thereby restricts the management of applications to the affected SD and to the AP owning the key set.

T.BRUTE-FORCE-SCP This Threat is covered by O.NO-KEY-REUSE which ensures that session keys can be used only once.

5.3.2 Organisational Security Policies

OSP.APPLICATIONS This OSP is enforced by the security objective for the operational environment of the TOE OE.APPLICATIONS.

OSP.AID-MANAGEMENT This OSP is directly enforced by the security objective for the operational environment of the TOE OE.AID-MANAGEMENT.

OSP.LOADING This OSP is enforced by the security objective for the operational environment of the TOE OE.LOADING.

OSP.SERVERS This OSP is enforced by the security objective for the operational environment of the TOE OE.SERVERS.

OSP.APSD-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.AP-KEYS.

OSP.ISD-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.ISD-KEYS.

OSP.KEY-GENERATION This OSP is enforced by the security objective for the operational environment of the TOE OE.KEY-GENERATION.

OSP.CASD-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.CA-KEYS.

OSP.KEY-CHANGE This OSP is enforced by the security objective for the operational environment of the TOE OE.KEY-CHANGE.

OSP.SECURITY-DOMAINS This OSP is enforced by the security objective for the TOE O.SECURITY-DOMAINS.

5.3.3 Assumptions

A.ISSUER This assumption is directly upheld by OE.ISSUER.

A.ADMIN This assumption is directly upheld by OE.ADMIN.

A.APPS-PROVIDER This assumption is directly upheld by OE.APPS-PROVIDER.

A.VERIFICATION-AUTHORITY This assumption is directly upheld by OE.VERIFICATION-AUTHORITY.

A.KEY-ESCROW This assumption is directly upheld by OE.KEY-ESCROW.

A.PERSONALISER This assumption is directly upheld by OE.PERSONALISER.

A.CONTROLLING-AUTHORITY This assumption is directly upheld by OE.CONTROLLING-AUTHORITY.

A.PRODUCTION This assumption is directly upheld by OE.PRODUCTION.

A.SCP-SUPP This assumption is directly upheld by OE.SCP-SUPP.

A.KEYS-PROT This assumption is directly upheld by OE.KEYS-PROT.

5.3.4 Rationale Tables of SPD and Security Objectives

Table 5-9: SPD and Security Objectives

SPDs	Security Objectives
T.COM-EXPLOIT	O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
T.UNAUTHORISED-CARD-MGMT	O.CARD-MANAGEMENT, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY, O.APPLI-AUTH, O.PRIVILEGES-MANAGEMENT, O.LC-MANAGEMENT, O.DOMAIN-RIGHTS
T.LIFE-CYCLE	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
T.BRUTE-FORCE-SCP	O.NO-KEY-REUSE
OSP.AID-MANAGEMENT	OE.AID-MANAGEMENT
OSP.LOADING	OE.LOADING
OSP.SERVERS	OE.SERVERS
OSP.APSD-KEYS	OE.AP-KEYS
OSP.ISD-KEYS	OE.ISD-KEYS
OSP.KEY-GENERATION	OE.KEY-GENERATION
OSP.CASD-KEYS	OE.CA-KEYS
OSP.KEY-CHANGE	OE.KEY-CHANGE
OSP.SECURITY-DOMAINS	O.SECURITY-DOMAINS
OSP.APPLICATIONS	OE.APPLICATIONS
A.ISSUER	OE.ISSUER
A.ADMIN	OE.ADMIN
A.APPS-PROVIDER	OE.APPS-PROVIDER
A.VERIFICATION-AUTHORITY	OE.VERIFICATION-AUTHORITY
A.KEY-ESCROW	OE.KEY-ESCROW
A.PERSONALISER	OE.PERSONALISER
A.CONTROLLING-AUTHORITY	OE.CONTROLLING-AUTHORITY
A.PRODUCTION	OE.PRODUCTION
A.SCP-SUPP	OE.SCP-SUPP
A.KEYS-PROT	OE.KEYS-PROT

6 Extended Security Requirements

6.1 Definition of the family FCS_RNG

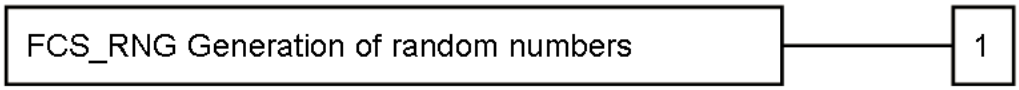
To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

6.2 FCS_RNG Generation of random numbers

Family behaviour: This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component levelling:



FCS_RNG.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management	There are no management activities are foreseen.
Audit	There are no actions are defined to be auditable.

FCS_RNG.1 Random numbers generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a **[selection: physical, non-physical true, deterministic, hybrid, hybrid deterministic]** random number generator **[selection: DRG.2, DRG.3, DRG.4, PTG.2, PTG.3, NTG.1] [AIS20] [AIS31]** that implements: **[assignment: list of security capabilities]**.

FCS_RNG.1.2 The TSF shall provide random numbers that meet **[assignment: a defined quality metric]**.

7 Security Requirements

7.1 Security Functional Requirements

This chapter provides the set of Security Functional Requirements (SFRs) the TOE has to enforce in order to fulfil the security objectives. One group of SFRs covers the Java Card System and comes from [PP-JC] (see section 7.1.1), while the other group of SFRs is added and covers the GlobalPlatform specification [GPCS] (see subsections of section 7.1.2).

The set of underlying security functional policies is the following:

Table 7-1: Security Functional Policies (SFP) of the core SE PP

[PP-JC] (see section 7.1.1)	Core SE PP (see section 7.1.2)	Description
Firewall access control SFP		Included in this PP by reference
ADEL access control SFP		Included in this PP by reference
JCVM information flow control SFP		Included in this PP by reference
Package Loading information flow control SFP	ELF Loading information flow control SFP	ELF Loading SFP replaces Package Loading SFP. Covers INSTALL and LOAD commands
--	Data & Key Loading information flow control SFP	New policy. Covers STORE DATA and PUT KEY commands.

7.1.1 Java Card System

This PP reuses all SFRs from [PP-JC]. The ST author must refer to the [PP-JC] to build the ST.

All SFRs with suffix /CM and /Installer defined in [PP-JC] are replaced by more specific and detailed requirements in section 7.1.2.

7.1.2 GlobalPlatform Card Management

This group of SFRs covers the following functions:

- SD and Application Life cycle management and transitions
- Privileges Management
- Secure Channel Protocols
- Trusted Framework.

Note: The deletion requirements for Applications and/or Executable Load Files are covered by the group ‘ADELG’ from [PP-JC] and are not repeated here. The [PP-JC] requirements are sufficient for this PP.

The Card Management requirements contain seven sub-groups of SFRs identified with the following suffixes:

- /GP-ELF for SFRs belonging to the ELF Loading information flow control policy
- /GP-KL for SFRs belonging to the Data & Key Loading information flow control policy
- /GP-LC for SFRs belonging to the Life Cycle management (states and transitions)

- /GP-PR for SFRs belonging to the Privileges assignment, management and transition
- /GP-SCP for SFRs belonging to the Secure Communication Protocols (SCPs)
- /GP-TF for SFRs belonging to the Trusted Framework scheme for inter-application communication
- /GP for common SFRs, mainly related to the security policies defined in /GP-ELF and /GP-KL.

7.1.2.1 ELF Loading Information Flow Control Policy

FDP_IFC.2/GP-ELF Complete information flow control

FDP_IFC.2.1/GP-ELF The TSF shall enforce the **ELF Loading information flow control SFP** on

- **Subjects: S.SD, S.CAD, S.OPEN**
- **Information: APDU commands INSTALL and LOAD, GlobalPlatform APIs for loading and installing ELF**

  and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/GP-ELF The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Application Note:

This SFR corresponds to FDP_IFC.2/CM of [PP-JC].

The subject S.SD can be the ISD, an APSD, or the CASD.

GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively.

FDP_IFF.1/GP-ELF Complete information flow control

FDP_IFF.1.1/GP-ELF The TSF shall enforce the **ELF Loading information flow control SFP** based on the following types of subject and information security attributes: **[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]**.

FDP_IFF.1.2/GP-ELF The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81], each with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **On receipt of INSTALL or LOAD commands, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **S.OPEN accepts an ELF only if its integrity and authenticity has been verified.**
- **[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].**

FDP_IFF.1.3/GP-ELF The TSF shall enforce the **[assignment: additional information flow control SFP rules].**

FDP_IFF.1.4/GP-ELF The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/GP-ELF The TSF shall explicitly deny an information flow based on the following rules:

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- **S.OPEN fails to verify the Card Life Cycle state**
- **S.OPEN fails to verify the SD privileges.**
- **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.SD fails to unwrap INSTALL or LOAD commands.**
- **[assignment: rules, based on security attributes, that explicitly deny information flows].**

Application Note:

This SFR refines and replaces FDP_IFF.1/CM of [PP-JC].

APDUs belonging to the policy ELF Loading information flow control SFP are described in the following references:

- For INSTALL, see [GPCS] section 11.5.
- For LOAD, see [GPCS] section 11.6.

The INSTALL and LOAD commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.

The minimum security level of INSTALL and LOAD is ‘AUTHENTICATED’ as defined in [GPCS] section 10.6.

For instance, Security attributes that can be used in FDP_IFF.1.1/GP-ELF are the authorisation status per Card Life Cycle State information, Privileges data, and the protection security levels of messages as defined in [GPCS] section 10.6: Entity authentication, Integrity and Data Origin authentication, Confidentiality.

For more details about the rules to be applied to each role of INSTALL command, refer to [GPCS] sections 9.3 and 3.4.

FDP_ITC.2/GP-ELF Import of user data with security attributes

FDP_ITC.2.1/GP-ELF The TSF shall enforce the **ELF Loading information flow control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/GP-ELF The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/GP-ELF The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/GP-ELF The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/GP-ELF The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **Referring to Java Card rules defined in [JCVM] and [JCRE]: ELF loading is allowed only if, for each dependent ELF, its AID attribute is equal to a resident ELF AID attribute, and the major (minor) Version attribute associated with the dependent ELF is less than or equal to the major (minor) Version attribute associated with the resident ELF**

- **[assignment: additional importation control rules].**

Application Note:

This SFR corresponds to FDP_ITC.2/Installer of [PP-JC].

Java Card rules are defined in [JCVM] sections 4.4 and 4.5 and [JCRE] section 11.

The TSF shall use the INSTALL data format and the LOAD data format when interpreting the user data from outside the TOE.

7.1.2.2 Data & Key Loading Information Flow Control Policy

FDP_IFC.2/GP-KL Complete information flow control

FDP_IFC.2.1/GP-KL The TSF shall enforce the **Data & Key Loading information flow control SFP** on

- **Subjects: S.SD, S.CAD, S.OPEN, Application**

- **Information: GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys**

  and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/GP-KL The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Application Note:

GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively.

The subject S.SD can be the ISD, an APSD, or the CASD.

FDP_IFF.1/GP-KL Complete information flow control

FDP_IFF.1.1/GP-KL The TSF shall enforce the **Data & Key Loading information flow control SFP** based on the following types of subject and information security attributes: **[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]**.

FDP_IFF.1.2/GP-KL The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81], each equipped with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the S.OPEN checks that the requesting S.SD has no restrictions for personalisation.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and prior to the command forwarding to the targeted Application or SD.**
- **[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].**

FDP_IFF.1.3/GP-KL The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/GP-KL The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/GP-KL The TSF shall explicitly deny an information flow based on the following rules:

- **S.OPEN fails to verify the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to unwrap STORE DATA or PUT KEY.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **[assignment: rules, based on security attributes, that explicitly deny information flows].**

Application Note:

APDUs belonging to the Data & Key Loading information flow control SFP are described in the following references:

- For PUT KEY, see [GPCS] section 11.8.
- For STORE DATA, see [GPCS] section 11.11.

The PUT KEY and STORE DATA commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.

The minimum security level of PUT KEY and STORE DATA is ‘AUTHENTICATED’ as defined in [GPCS] section 10.6.

For instance, Security attributes that can be used in FDP_IFF.1.1/GP-KL are the authorisation status per Card Life Cycle State information, Privileges data, and the protection security levels of messages as defined in [GPCS] section 10.6: Entity authentication, Integrity and Data Origin authentication, Confidentiality.

For more details about Key Access Conditions, Data and Key Management, refer to [GPCS] sections 7.5.2 and 7.6.

FDP_ITC.2/GP-KL Import of user data with security attributes

FDP_ITC.2.1/GP-KL The TSF shall enforce the **Data & Key Loading information flow control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/GP-KL The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/GP-KL The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/GP-KL The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/GP-KL The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **The algorithms and key sizes of the imported keys shall be supported by the SE**
- **[assignment: additional importation control rules].**

Application Note:

The algorithms and key sizes of the imported keys shall be supported by the Card as specified in [GPCS] Appendices B and C.

PUT KEY and STORE DATA are described in [GPCS] sections 11.8 and 11.11.

7.1.2.3 Life Cycle Management

FMT_MTD.1/GP-LC Management of TSF Data

FMT_MTD.1.1/GP-LC The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorised identified roles]**.

Table 7-2: Life Cycle Management Operations, Data, and Roles

Operations (APDUs or APIs)	List of TSF Data: (Life Cycle State and Transitions)	Authorised Identified Roles
Query (GET STATUS)	Card Life Cycle State information	ISD on behalf of the Issuer, Supplementary SD (SSD) on behalf of AP
	Application or SSD Life Cycle State information	ISD on behalf of the Issuer, AP owning the corresponding SSD or Application
	Executable Load Files Life Cycle State information	ISD on behalf of the Issuer, AP owning the corresponding ELF
	Executable Load Files and Executable Modules Life Cycle State information	ISD on behalf of the Issuer, AP owning the corresponding ELF and Modules

Operations (APDUs or APIs)	List of TSF Data: (Life Cycle State and Transitions)	Authorised Identified Roles
Change_default (SET STATUS)	Card Life Cycle State information and transitions as defined in [GPCS]	ISD on behalf of the Issuer
	Application or SSD Life Cycle State information and transitions as defined in [GPCS]	AP owning the corresponding SSD or Application
	SD and its associated Applications Life Cycle State information	AP owning the corresponding SSD and its Applications

Application Note:

Refer to the following sections in [GPCS] for additional details about Life Cycle:

- Card Life Cycle states and transitions are described in [GPCS] section 5.1.
- The Executable Load File/ Executable Module Life Cycle is described in [GPCS] section 5.2.
- Application and Security Domain Life Cycle states and transitions are described in [GPCS] section 5.3.
- Authorised commands per Card Life Cycle state are detailed in [GPCS] Table 11-1.
- The GET STATUS APDU command used to query Life Cycle state information of an ISD, Executable Load File, Executable Module, Application, or SD is described in [GPCS] section 11.4.
- The SET STATUS APDU command used to change the Life Cycle state information of an ISD, Supplementary SD, or Application is described in [GPCS] section 11.10.
- The minimum security level for SET STATUS and GET STATUS is 'AUTHENTICATED' as defined in [GPCS] section 10.6.

7.1.2.4 Privileges Management

FMT_MTD.1/GP-PR Management of TSF Data

FMT_MTD.1.1/GP-PR The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **[assignment: the authorised identified roles]**.

Table 7-3: Privileges Management Operations, Data, and Roles

Operations (APDUs or APIs)	List of TSF Data: Privileges	Authorised Identified Roles
Modify (INSTALL [for registry update])	Privileges of an Application or SSD	SD processing the command shall be an ancestor SD with the AM privilege, or an SD with DM privilege under an ancestor SD with AM privilege
	Privileges of ISD	Only ISD

Application Note: The 'Privileges Management' requirements cover all Privileges Assignment, Management, and Transition as defined in [GP CIC] section 3.1.1 and [GPCS] section 6.6.

7.1.2.5 Secure Communication

The purpose of an SCP is to authenticate the on-card and off-card entities and to protect the data exchanged between them with regard to Authenticity, Integrity, and/or Confidentiality.

The Secure Communication requirements cover all SCPs defined by [GPCS et al.]:

- The symmetric key Secure Channel Protocol '03' defined in [Amd D] includes services similar to Secure Channel Protocol '02' [GPCS]; however, it uses AES rather than DES cryptography.
- The asymmetric key Secure Channel Protocol '10' [GPCS] offers authentication services using an RSA-based Public Key Infrastructure (PKI) and secure messaging protection of commands and responses using symmetric cryptography.
- The asymmetric key Secure Channel Protocol '11' defined in [Amd F] offers authentication services using an ECC-based Public Key Infrastructure (PKI) and secure messaging protection of commands and responses based on SCP03.
- The Secure Channel Protocol '22' defined in [Amd G] is a Secure Channel and key establishment protocol, collectively known as the Opacity Secure Channel establishment method.
- The Secure Channel Protocol '21' defined in [GP PF] Annex D enforces privacy requirements.
- The Secure Channel Protocol '80' supports the Over-The-Air security scheme defined in [TS 102 225], [TS 102 226].
- The Secure Channel Protocol '81' defined in [Amd B] supports an Over-The-Air security scheme based on the usage of both HTTP and Pre-Shared Key TLS protocols.

APDU commands belonging to SCPs are defined in the following references:

- SCP02 – [GPCS] Annex E
- SCP10 – [GPCS] Annex F
- SCP03 – [Amd D] section 7
- SCP11 – [Amd F] section 6
- SCP21 – [GP PF] Annex D
- SCP22 – [Amd G] section 6
- SCP80 – [TS 102 225] and [TS 102 226]
- SCP81 – [Amd B].

The following references give details about the rules to be applied to SCPs:

- Rules that apply to all Secure Channel Protocols as defined in [GPCS] Chapter 10.
- Rules for handling Security Levels in [GPCS] section 10.6
- SCP02 protocol rules as defined in [GPCS] section E.1.6
- SCP10 protocol rules as defined in [GPCS] section F.1.6
- SCP03 protocol rules as defined in [Amd D] section 5.6
- SCP11 protocol rules as defined in [Amd F] section 4.8
- SCP21 protocol rules as defined in [GP PF] Annex D
- SCP22 protocol rules as defined in [Amd G] section 4
- SCP80 protocol rules as defined in [TS 102 225] and [TS 102 226]

- SCP81 protocol rules as defined in [Amd B] section 3.

Recommendations for appropriate cryptographic algorithms, key sizes and standards are given in [GP Crypto]. These are aligned with the recommendations issued by NIST [NIST 800-131A], SOG-IS [SOG-IS_ACM], BSI [TR 02102] and ANSSI [ANSSI-RGS].

FCS_RNG.1/GP-SCP Random numbers generation

FCS_RNG.1.1/GP-SCP The TSF shall provide a **[selection: physical, non-physical true, deterministic, hybrid, hybrid deterministic]** random number generator **[selection: DRG.2, DRG.3, DRG.4, PTG.2, PTG.3, NTG.1] [AIS20] [AIS31]** that implements: **[assignment: list of security capabilities]**.

FCS_RNG.1.2/GP-SCP The TSF shall provide random numbers that meet **[assignment: a defined quality metric]**.

Application Note:

This SFR belongs to SCP22 generating an ephemeral EC key pair.

This SFR corresponds to FCS_RNG.1 of [PP-JC], applied to SCP22 (this is why it has been renamed).

FCS_CKM.1/GP-SCP Cryptographic key generation

FCS_CKM.1.1/GP-SCP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- The session key generation within SCP02 is described in [GPCS] section E.4.1.
- The session key generation within SCP10 is described in [GPCS] section F.1.2.
- The session key generation within SCP03 is described in [Amd D] section 6.2.1.
- The session key generation within SCP11 is described in [Amd F] section 5.2.

FCS_COP.1/GP-SCP Cryptographic operation

FCS_COP.1.1/GP-SCP The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**

Application Note:

- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].
- The ST writer may define one FCS_COP.1 for all cryptographic operations implemented by the TOE or one FCS_COP.1 per operation or SCP.

- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.

Table 7-4: Cryptographic Operations Covering the SCPs Defined by GP

SCP Protocol	Operation	Algorithm	Key Sizes	Recommended Standards
SCP02	MAC Generation/ Verification	H-MAC, CMAC using TDES	112 bits	[FIPS 198]
SCP02	Symmetric Encryption/ Decryption	TDES in CBC mode	112 bits	[NIST 800-67], [NIST 800-38A]
SCP02	Key Derivation	HMAC-based KDF, CMAC-based KDF using TDES	112 bits	[NIST 800-108], [FIPS 198]
SCP03, SCP11	Symmetric Encryption/ Decryption	AES in CBC mode	128, 192, or 256 bits	[FIPS 197], [NIST 800-38A], and [FIPS 140-2]
SCP03, SCP22	MAC Generation/ Verification	CMAC AES	128, 192, or 256 bits	[NIST 800-38B] and [FIPS 140-2]
SCP03, SCP22	Key Derivation	CMAC-based KDF using AES	128, 192, or 256 bits	[NIST 800-108], [NIST 800-38B]
SCP10	Asymmetric Encryption/ Decryption	RSAES-PKCS1-v1_5 (Deprecated), RSAES-OAEP	1024 to 4096 bits	[PKCS#1]
SCP02, SCP03, SCP10, SCP11	Hash Computing	SHA-256, SHA-384, SHA-512		[ISO 10118-3] and [FIPS 180-4]
SCP22	Authenticated Encryption (AEAD)	AES	128, 192, or 256 bits	[ISO 19772]
SCP22	Secure Messaging	ECDH : Opacity ZKM and Opacity FS	256, 384, 512, 521 bits	[ANSI 504-1], [NIST 800-73-4]
SCP22	Asymmetric Encryption/ Decryption	ECC	256, 384, 512, 521 bits	[RFC 5639]
SCP22	Digital Signature	RSA with SHA-256, SHA-384, SHA-512	1024 to 4096 bits	[PKCS#1]
SCP22	Digital Signature	ECDSA with SHA-256, SHA-384, SHA-512	256, 384, 512, 521 bits	[ANSI X9.62], [FIPS 186-4]

SCP Protocol	Operation	Algorithm	Key Sizes	Recommended Standards
SCP22	Key Agreement	ECKA-EG	≥ 256 bits	[NIST 800-56A]
SCP21	Privacy-enabled Secure Channel (Prevention of privacy leakage)	PACE (Password Authentication Connection Establishment)		[419 212] part 1 section 9, [ICAO 9303]
SCP21	Privacy-enabled Secure Channel (Prevention of privacy leakage)	mEAC (modular Extended Access Control) which uses EAC V1 or EAC V2		[419 212] part 1 section 8.8
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 112 bits AES: 128, 192, or 256 bits	[TS 102 225], [TS 102 226]
SCP81	Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_3DES_EDE_CBC_SHA TLS_PSK_WITH_AES_128_CBC_SHA TLS_PSK_WITH_NULL_SHA TLS_PSK_WITH_AES_128_CBC_SHA256 TLS_PSK_WITH_NULL_SHA256		[Amd B] section 3.3.2

See recommendations 1 to 4 from Table 2-1.

7.1.2.6 Trusted Framework

FTP_TRP.1/GP-TF Trusted Path

FTP_TRP.1.1/GP-TF The TSF shall provide a communication path between itself and **the Target Application and the Receiving SD** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]]**.

FTP_TRP.1.2/GP-TF The TSF shall permit **the Receiving SD with the Trusted Path privilege, the Trusted Framework, and the Target Application** to initiate communication via the trusted path.

FTP_TRP.1.3/GP-TF The TSF shall require the use of the trusted path for:

- **Application personalisation: the GlobalPlatform Trusted Framework for inter-application communication forwards the unwrapped command (STORE DATA) to the Target Application indicated by the Receiving SD through its GlobalPlatform Application interface.**

7.1.2.7 Common SFRs

FMT_MSA.1/GP Management of security attributes

FMT_MSA.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **[assignment: list of security attributes]** to **[assignment: the authorised identified roles].**

Table 7-5: GlobalPlatform Common Operations, Security Attributes, and Roles

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorised Identified Roles with Privileges
DELETE Executable Load File	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Executable Load File and related Application(s)	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Application	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Key	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
INSTALL	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
INSTALL [for personalisation]	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
LOAD	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
PUT KEY	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
SELECT	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED (If an SD does have the Final Application privilege)	ISD, AM SD, DM SD, SD with Final Application privilege
SET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, CARD_LOCKED, or TERMINATED	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD

Table 7-6: SCP02 Operations, Security Attributes, and Roles

Operations: SCP02 Commands	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
INITIALIZE UPDATE	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	None	ISD, AM SD, DM SD, SD
EXTERNAL AUTHENTICATE		C-MAC	

Table 7-7: SCP10 Operations, Security Attributes, and Roles

Operations: SCP10 Commands	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
EXTERNAL AUTHENTICATE	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	[GPCS] Table F-14	ISD, AM SD, DM SD, SD
GET CHALLENGE			
GET DATA [certificate]			
INTERNAL AUTHENTICATE			
MANAGE SECURITY ENVIRONMENT			
PERFORM SECURITY OPERATION [decipher]			
PERFORM SECURITY OPERATION [verify certificate]			

Table 7-8: SCP11 Operations, Security Attributes, and Roles

Operations: SCP11 Commands	Used by	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
GET DATA (ECKA Certificate)	SCP11a and b	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	None	ISD, AM SD, DM SD, SD
PERFORM SECURITY OPERATION	SCP11a		None	
MUTUAL AUTHENTICATE	SCP11a		AUTHENTICATED or ANY_AUTHENTICATED	
INTERNAL AUTHENTICATE	SCP11b		AUTHENTICATED or ANY_AUTHENTICATED	
STORE DATA (ECKA Certificate)	SCP11a and b		None	
STORE DATA (Whitelist)	SCP11a		None	
VERIFY PIN	SCP11b		None	

Table 7-9: SCP21 Operations, Security Attributes, and Roles

Operations: SCP21 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
PACE	Defined in [ICAO 9303] and [419 212] part 1 section 9		ISD, AM SD, DM SD, SD
EAC V1	Defined in [419 212] part 1 section 8.8		
PACE + EAC V2	Defined in [419 212] part 1 sections 8.8 and 9		

Table 7-10: SCP22 Operations, Security Attributes, and Roles

Operations: SCP22 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
SELECT MF	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	None	ISD, AM SD, DM SD, SD
SELECT FILE [by FID] (other than SELECT MF)	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
READ BINARY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
READ RECORD	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD

Operations: SCP22 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
GENERAL AUTHENTICATE	OP_READY, INITIALIZED, SECURED	AUTHENTICATED or ANY_AUTHENTICATED	ISD, AM SD, DM SD, SD

Table 7-11: SCP80 Operations, Security Attributes, and Roles

Operations: SCP80 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
Remote File Management Commands SELECT UPDATE BINARY UPDATE RECORD SEARCH RECORD INCREASE VERIFY PIN CHANGE PIN DISABLE PIN ENABLE PIN UNBLOCK PIN DEACTIVATE FILE ACTIVATE FILE READ BINARY READ RECORD CREATE FILE DELETE FILE RESIZE FILE SET DATA RETRIEVE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]
Remote Applet Management Commands DELETE SET STATUS INSTALL LOAD PUT KEY GET STATUS GET DATA STORE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]

Table 7-12: SCP81 Operations, Security Attributes, and Roles

Operations: SCP81 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
PUT KEY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, CARD_LOCKED, or TERMINATED ISD, AM SD, DM SD, SD	None	ISD, AM SD, DM SD, SD

Legend:

ISD: Issuer Security Domain

AM SD: Security Domain with Authorised Management privilege

DM SD: Security Domain with Delegated Management privilege

SD: Other Security Domain

Application Note:

This SFR refines FMT_MSA.1/CM of [PP-JC]. It is extended to cover Data and Key loading Policy.

The authorised identified roles could be off-card or on-card entities as defined in FMT_SMR.1/GP.

FMT_MSA.3/GP Security attribute initialization

FMT_MSA.3.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/GP The TSF shall allow the **[assignment: authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

This SFR refines FMT_MSA.1/CM of [PP-JC]. It is extended to cover the Data and Key loading Policy.

The authorised identified roles could be off-card or on-card entities as defined in FMT_SMR.1/GP.

FMT_SMR.1/GP Security roles

FMT_SMR.1.1/GP The TSF shall maintain the roles:

- **On-card: S.OPEN, S.SD (e.g. ISD, APSD, CASD), Application**

- **Off-card: Issuer, Users (e.g. VA, AP, CA) owning SDs.**

FMT_SMR.1.2/GP The TSF shall be able to associate users with roles.

Application Note:

This SFR corresponds to FMT_SMR.1/Installer and FMT_SMR.1/CM of [PP-JC], applied to roles involved in card content management operations (this is why it has been renamed).

FMT_SMF.1/GP Specification of Management Functions

FMT_SMF.1.1/GP The TSF shall be capable of performing the following management functions **specified in [GPCS]:**

- **Card and Application Security Management as defined in [GPCS]: Life Cycle, Privileges, Application/SD Locking and Unlocking, Card Locking and Unlocking, Card Termination, Application Status interrogation, Card Status Interrogation, command dispatch, Operational Velocity Checking, and Tracing and Event Logging.**

- **Management functions (Secure Channel Initiation/Operation/Termination) related to SCPs as defined in [GPCS].**

Application Note:

This SFR corresponds to FMT_SMF.1/CM of [PP-JC], applied to card content management operations (this is why it has been renamed).

Management functions related to SCPs are defined in [GPCS] Chapter 10.

FPT_RCV.3/GP Automated recovery without undue loss

FPT_RCV.3.1/GP When automated recovery from **[assignment: list of failures/service discontinuities during card content management operations]** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/GP For **[assignment: list of failures/service discontinuities during card content management operations]** the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/GP The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **[assignment: quantification]** for loss of TSF data or objects under the control of the TSF.

FPT_RCV.3.4/GP The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

Application Note:

This SFR corresponds to FPT_RCV.3/Installer of [PP-JC], applied to card content management operations (this is why it has been renamed).

FPT_RCV.3.1 and FPT_RCV.3.2 are complementary requirements. The first allows to specify a maintenance mode through FMT_SMF.1 and the second allows to state which types of failure or service discontinuity require automatic recovery procedures.

Note: If there are no failures defined, there is no requirement to define a maintenance mode.

Examples of failures include interruption of the installation of an Executable Load File, interruption of a package/application deletion, loss of the integrity of Executable Load File, and error during linking of an executable Load File with the Files already present in the card. The behaviour of the TSF is implementation-dependent.

For FPT_RCV.3.3, the acceptable loss may refer to a transaction mechanism used in card content operations. For instance, loss of the Executable Load File upon installation failure, or loss of newly created Java Card objects upon Application instance failure.

FPT_FLS.1/GP Failure with preservation of secure state

FPT_FLS.1.1/GP The TSF shall preserve a secure state when the following types of failures occur:

- **S.OPEN fails to load/install an Executable Load File / Application instance.**
- **S.SD fails to load SD/Application data and keys.**
- **S.OPEN fails to verify/change the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **[assignment: list of additional types of failures].**

Application Note:

This SFR extends FPT_FLS.1/Installer of [PP-JC] to include the failures that may occur during the loading of SD/Application keys and data.

Refer to [JCRE] section 11.1.5 and [GPCS] sections 11.5, 11.6, 11.8, and 11.11 for additional details.

FPT_TDC.1/GP Inter-TSF basic TSF data consistency

FPT_TDC.1.1/GP The TSF shall provide the capability to consistently interpret **ELFs, SD/Application data and keys, data used to implement a Secure Channel, [assignment: list of TSF data types]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/GP The TSF shall use **the list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card, [assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application Note:

The list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card are defined in [GPCS] sections 11.5, 11.6, 11.8, and 11.11.

FTP_ITC.1/GP Inter-TSF trusted channel

FTP_ITC.1.1/GP The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/GP The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/GP The TSF shall initiate communication via the trusted channel for:

- **APDU commands sent to the card within a Secure Channel Session**
- **When loading/installing a new ELF on the card**
- **When transmitting and loading sensitive data to the card using STORE DATA or PUT KEY commands**
- **When deleting ELFs, Applications, or Keys**
- **[assignment: list of functions for which a trusted channel is required].**

Application Note:

This SFR corresponds to FTP_ITC.1/CM of [PP-JC], applied where APDU command and response integrity and/or confidentiality protection through a Secure Channel are required.

FCO_NRO.2/GP Enforced proof of origin

FCO_NRO.2.1/GP The TSF shall enforce the generation of evidence of origin for transmitted **[assignment: list of information types]** at all times.

Refinement

The TSF shall be able to generate an evidence of origin at all times for 'Executable Load Files, SD/Application data and keys' received from the off-card entity (originator of transmitted data) that communicates with the card.

FCO_NRO.2.2/GP The TSF shall be able to relate the **[assignment: list of attributes]** of the originator of the information, and the **[assignment: list of information fields]** of the information to which the evidence applies.

Refinement

The TSF shall be able to load 'Executable Load Files, SD/Application data and keys' to the card with associated security attributes (the identity of the originator, the destination) such that the evidence of origin can be verified.

FCO_NRO.2.3/GP The TSF shall provide a capability to verify the evidence of origin of information to **the off-card entity (recipient of the evidence of origin) who requested that verification** given **[assignment: limitations on the evidence of origin]**.

Application Note:

This SFR extends FCO_NRO.2/CM of [PP-JC] to cover the SD/Application data and keys transmitted and loaded to the card via STORE DATA and PUT KEY commands.

The exact limitations for the evidence of origin are implementation-dependent. In most of the implementations, the card manager performs an immediate verification of the origin of the package using an electronic signature mechanism, and no evidence is kept on the card for future verifications.

FIA_UID.1/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **[assignment: list of TSF-mediated actions]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/GP The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

This SFR corresponds to FIA_UID.1/CM of [PP-JC].

The list of TSF-mediated actions is implementation-dependent, but ELF installation, SD/Application data and keys loading require user identification. For instance, the list of TSF-mediated actions may be:

- Application selection,
- Initializing a Secure Channel with the card,
- Requesting data that identifies the card or off-card entities.

FDP_UIT.1/GP Basic data exchange integrity

FDP_UIT.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to **[selection: transmit, receive]** user data in a manner protected from **modification, deletion, insertion, replay** errors.

FDP_UIT.1.2/GP The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion, replay** has occurred.

Application Note:

This SFR extends FDP_UIT.1/CM of [PP-JC] to cover the integrity protection of SD/Application data and keys.

This SFR applies where APDU command and response integrity protection is required. For instance: INSTALL, LOAD, STORE DATA and PUT KEY commands.

FDP_ROL.1/GP Basic rollback

FDP_ROL.1.1/GP The TSF shall enforce **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to permit the rollback of the **installation, loading, or removal operation** on the **executable files, application instances, SD/Application data and keys**.

FDP_ROL.1.2/GP The TSF shall permit operations to be rolled back within the **boundary limit:**

- **Until the Executable File or application instance has been added to or removed from the applet's registry.**
- **Until SD/Application data or keys have been added to or removed from SD or Application.**

FDP_UCT.1/GP Basic data exchange confidentiality

FDP_UCT.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to **[selection: transmit, receive]** user data in a manner protected from unauthorised disclosure.

Application Note:

This SFR applies where APDU command and response confidentiality protection is required. For example, the sensitive data (e.g. secret keys) shall always be transmitted as confidential data.

FPR_UNO.1/GP Unobservability

FPR_UNO.1.1/GP The TSF shall ensure that **SDs and Applications** are unable to observe the operation: **keys or data import (PUT KEY or STORE DATA), encryption, decryption, signature generation and verification, [assignment: list of operations]** on **keys and data** by **the OPEN or any other SD or Application**.

FIA_UAU.1/GP Timing of authentication

FIA_UAU.1.1/GP The TSF shall allow **the TSF mediated actions listed in FIA_UID.1/GP** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/GP The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/GP Single-use authentication mechanisms

FIA_UAU.4.1/GP The TSF shall prevent reuse of authentication data related to **the authentication mechanism used to open a secure communication channel with the card**.

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]** unsuccessful authentication attempts occur related to **the authentication of the origin of a card management operation command**.

FIA_AFL.1.2/GP When the defined number of unsuccessful authentication attempts has been **met or surpassed**, the TSF shall **close the Secure Channel**.

FMT_MTD.3/GP Secure TSF Data

FMT_MTD.3.1/GP The TSF shall ensure that only secure values are accepted for **Life Cycle states, Security Levels and Privileges in the GlobalPlatform Registry.**

7.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

7.3 Security Requirements Rationale

7.3.1 Objectives

7.3.1.1 Java Card System

The ST Author is referred to the Security Requirements Rationale in the Protection Profile JCP [PP-JC], section 7.4. This PP extends those rationales as follows:

O.LOAD The following requirements contribute to fulfil the objective:

- FCO_NRO.2/GP enforces the evidence of the origin during the loading of Executable Load Files, SD/Application data and keys.
- FDP_IFC.2/GP-ELF and FDP_IFF.1/GP-ELF enforce the ELF loading information flow control policy for managing, authenticating, and protecting the card management commands.
- FDP_UIT.1/GP ensures the integrity of the card management operations.
- FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, these SFRs specify the actions being performed before the authentication of the origin of the received APDU commands takes place.
- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.

O.INSTALL The following requirements contribute to fulfil the objective:

- FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs.
- FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting an Executable File / application instance.

- FPT_RCV.3/GP ensures safe recovery from failure.

O.DELETION The following requirements contribute to fulfil the objective:

- FPT_RCV.3/GP ensures safe recovery from failure.

O.RESOURCES The following requirements contribute to fulfil the objective:

- FPT_RCV.3/GP ensures safe recovery from failure.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the corresponding commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider and the Controlling Authority roles and specifies the authorised roles that are allowed to send and authenticate the card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.
- FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting of an Executable File / application instance.

O.ALARM The following requirements contribute to fulfil the objective:

- FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting an Executable File / application instance.

O.OPERATE The following requirements contribute to fulfil the objective:

- FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting an Executable File / application instance.
- FPT_RCV.3/GP ensures safe recovery from failure.

O.KEY-MNGT The following requirements contribute to fulfil the objective:

- FPT_TDC.1/GP specifies requirements preventing any possible misinterpretation of the Security Domain keys used to implement a Secure Channel when those are loaded form the off-card entity.
- FCS_CKM.1/GP-SCP specifies the algorithm, key sizes, and standards used for the generation of session keys.
- FCS_COP.1/GP-SCP specifies the cryptographic operations and algorithms that shall be used to establish a Secure Channel to protect the card management commands.

O.CIPHER The following requirements contribute to fulfil the objective:

- FCS_CKM.1/GP-SCP specifies the algorithm, key sizes, and standards used for the generation of session keys.
- FCS_COP.1/GP-SCP specifies the cryptographic operations and algorithms that shall be used to establish a Secure Channel to protect the card management commands.

O.SID The following requirements contribute to fulfil the objective:

- FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs.
- FDP_ITC.2/GP-KL enforces the Data & Key information flow policy when importing keys and data.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
    - ensure the authenticity, integrity, and/or confidentiality of card management commands;
    - enforce the TOE Life cycle management and transitions.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.

O.FIREWALL The following requirements contribute to fulfil the objective:

- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
    - ensure the authenticity, integrity, and/or confidentiality of card management commands;
    - enforce the TOE Life cycle management and transitions.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity and confidentiality.
- FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs.
- FDP_ITC.2/GP-KL enforces the Data & Key information flow policy when importing keys and data.

O.RNG The following requirement contributes to fulfil the objective:

- FCS_RNG.1/GP-SCP ensures the cryptographic quality of random number generation.

7.3.1.2 Card Management

O.CARD-MANAGEMENT The following requirements contribute to fulfil the objective:

- FDP_UIT.1/GP ensures the integrity of card management operations.
- FDP_UCT.1/GP ensures the confidentiality of card management operations.
- FDP_ROL.1/GP ensures the rollback of the installation or removal operation on the executable files and application instances.
- FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs.
- FDP_ITC.2/GP-KL enforces the Data & Key information flow policy when importing keys and data.
- FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting an Executable File / application instance.

- FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the information flow control policy for managing, authenticating, and protecting the Card management commands and responses between off-card and on-card entities.
- FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, these SFRs specify the actions being performed before the authentication of the origin of the received APDU commands takes place.
- FCO_NRO.2/GP enforces the evidence of the origin during the loading of Executable Load Files, SD/Application data and keys.
- FPR_UNO.1/GP enforces the invisibility of the imported keys and the encryption, decryption, signature generation and verification cryptographic mechanisms on SD/Application keys and data.
- FPT_TDC.1/GP specifies requirements preventing any possible misinterpretation of the Security Domain keys used to implement a Secure Channel when those are loaded from the off-card entity.
- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
    - ensure the authenticity, integrity, and/or confidentiality of card management commands;
    - enforce the TOE Life cycle management and transitions.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.
- FPT_RCV.3/GP ensures safe recovery from failure.
- FIA_AFL.1/GP supports the objective by bounding the number of signatures that the attacker may try to attach to a message to authenticate its origin.

O.DOMAIN-RIGHTS The following requirements contribute to fulfil the objective:

- FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the ELF, data and keys loading information flow control policy for managing, authenticating and protecting the Card management commands and responses between off-card and on-card entities.
- FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, these SFRs specify the actions being performed before the authentication of the origin of the received APDU commands takes place.
- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
- FCO_NRO.2/GP enforces the evidence of the origin during the loading of Executable Load Files, SD/Application data and keys.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
    - ensure the authenticity, integrity, and/or confidentiality of card management commands;
    - enforce the TOE Life cycle management and transitions.

- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.

O.APPLI-AUTH The following requirements contribute to fulfil the objective:

- FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF enforce the ELF loading information flow control policy for managing, authenticating, and protecting the Card management commands.
- FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs.
- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
    - ensure the authenticity, integrity, and/or confidentiality of card management commands;
    - enforce the TOE Life cycle management and transitions.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.

O.SECURITY-DOMAINS The following requirements contribute to fulfil the objective:

- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
    - Ensure the authenticity, integrity, and/or confidentiality of card management commands;
    - enforce the TOE Life cycle management and transitions.

O.LC-MANAGEMENT The following requirements contribute to fulfil the objective:

- FMT_MTD.1/GP-LC, FMT_MTD.3/GP cover Life Cycle Management functions and transitions.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:

- ensure the authenticity, integrity, and/or confidentiality of card management commands;
- enforce the TOE Life cycle management and transitions.

7.3.1.3 Privileges Management

O.PRIVILEGES-MANAGEMENT The following requirements contribute to fulfil the objective:

- FMT_MTD.1/GP-PR, FMT_MTD.3/GP cover Privileges Assignment and Management functions.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity and confidentiality.

7.3.1.4 Secure Communication

O.COMM-AUTH The following requirements contribute to fulfil the objective:

- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity and confidentiality.
- FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the ELF, data and keys loading information flow control policy for managing, authenticating, and protecting the Card management commands and responses between off-card and on-card entities.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
  - ensure the authenticity, integrity, and/or confidentiality of card management commands;
  - enforce the TOE Life cycle management and transitions.
- FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, these SFRs specify the actions being performed before the authentication of the origin of the received APDU commands takes place.
- FCS_COP.1/GP-SCP specifies the cryptographic operations and algorithms that shall be applied for the authorisation of the card management commands.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.

O.COMM-INTEGRITY The following requirements contribute to fulfil the objective:

- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.

- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.
- FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the ELF, data and keys loading information flow control policy for managing, authenticating, and protecting the Card management commands and responses between off-card and on-card entities.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
  - ensure the authenticity, integrity, and/or confidentiality of card management commands;
  - enforce the TOE Life cycle management and transitions.
- FCS_COP.1/GP-SCP specifies the cryptographic operations and algorithms that shall be used to ensure the integrity of the card management commands.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.

O.COMM-CONFIDENTIALITY The following requirements contribute to fulfil the objective:

- FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality.
- FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the ELF, data and keys loading information flow control policy for managing, authenticating, and protecting the Card management commands and responses between off-card and on-card entities.
- FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to:
  - ensure the authenticity, integrity, and/or confidentiality of card management commands;
  - enforce the TOE Life cycle management and transitions.
- FCS_COP.1/GP-SCP specifies the cryptographic operations and algorithms that shall be used to ensure the confidentiality of the card management commands (decryption of the card management commands).

O.NO-KEY-REUSE The following requirements contribute to fulfil the objective:

- FIA_UAU.4/GP enforces the objective by requesting the TSF to prevent the reuse of authentication data related to the implementation of Secure Channels.
- FIA_AFL.1/GP supports the objective by bounding the number of signatures that the attacker may try to attach to a message to authenticate its origin.

7.3.2 Rationale Tables of Security Objectives and SFRs

Table 7-13: Security Objectives and SFRs

Security Objectives	SFRs
O.LOAD	FCO_NRO.2/GP, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_UIT.1/GP, FIA_UID.1/GP, FTP_ITC.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP
O.INSTALL	FDP_ITC.2/GP-ELF, FPT_FLS.1/GP, FPT_RCV.3/GP
O.DELETION	FPT_RCV.3/GP
O.RESOURCES	FPT_RCV.3/GP, FMT_SMR.1/GP, FMT_SMF.1/GP, FPT_FLS.1/GP
O.ALARM	FPT_FLS.1/GP
O.OPERATE	FPT_FLS.1/GP, FPT_RCV.3/GP
O.KEY-MNGT	FPT_TDC.1/GP, FCS_CKM.1/GP-SCP, FCS_COP.1/GP-SCP
O.CIPHER	FCS_CKM.1/GP-SCP, FCS_COP.1/GP-SCP
O.SID	FDP_ITC.2/GP-ELF, FDP_ITC.2/GP-KL, FMT_SMR.1/GP, FMT_SMF.1/GP, FMT_MSA.1/GP, FMT_MSA.3/GP
O.FIREWALL	FMT_SMR.1/GP, FMT_SMF.1/GP, FDP_ITC.2/GP-ELF, FDP_ITC.2/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP
O.RNG	FCS_RNG.1/GP-SCP
O.CARD-MANAGEMENT	FPT_FLS.1/GP, FDP_ROL.1/GP, FCO_NRO.2/GP, FMT_SMR.1/GP, FMT_SMF.1/GP, FDP_ITC.2/GP-ELF, FDP_ITC.2/GP-KL, FPT_RCV.3/GP, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FIA_UID.1/GP, FIA_AFL.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FTP_ITC.1/GP, FPR_UNO.1/GP, FPT_TDC.1/GP, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP
O.DOMAIN-RIGHTS	FMT_SMR.1/GP, FMT_SMF.1/GP, FCO_NRO.2/GP, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FIA_UID.1/GP, FIA_AFL.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FTP_ITC.1/GP, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP
O.APPLI-AUTH	FMT_SMR.1/GP, FDP_ITC.2/GP-ELF, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FTP_ITC.1/GP, FMT_MSA.1/GP, FMT_MSA.3/GP
O.SECURITY-DOMAINS	FMT_SMR.1/GP, FMT_SMF.1/GP, FMT_MSA.1/GP, FMT_MSA.3/GP
O.LC-MANAGEMENT	FMT_MTD.1/GP-LC, FMT_MTD.3/GP
O.PRIVILEGES-MANAGEMENT	FMT_SMR.1/GP, FMT_SMF.1/GP, FMT_MTD.1/GP-PR, FMT_MTD.3/GP
O.COMM-AUTH	FMT_SMR.1/GP, FMT_SMF.1/GP, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FIA_UID.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FTP_ITC.1/GP, FCS_COP.1/GP-SCP, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP

Security Objectives	SFRs
O.COMM-INTEGRITY	FMT_SMR.1/GP, FMT_SMF.1/GP, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FTP_ITC.1/GP, FCS_COP.1/GP-SCP, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP
O.COMM-CONFIDENTIALITY	FMT_SMR.1/GP, FMT_SMF.1/GP, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FTP_ITC.1/GP, FCS_COP.1/GP-SCP, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP
O.NO-KEY-REUSE	FIA_AFL.1/GP, FIA_UAU.4/GP

7.3.3 Dependencies

7.3.3.1 SFRs Dependencies

Table 7-14: SFRs Dependencies

SFRs	CC Dependencies	Satisfied Dependencies
FDP_UCT.1/GP	(FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path) (FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FPT_TDC.1/GP	No Dependencies	No Dependencies
FDP_ROL.1/GP	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL
FPR_UNO.1/GP	No Dependencies	No Dependencies
FIA_UAU.1/GP	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FIA_UAU.4/GP	No Dependencies	No Dependencies
FIA_AFL.1/GP	FIA_UAU.1 Timing of authentication	FIA_UAU.1/GP
FMT_MTD.3/GP	FMT_MTD.1 Management of TSF data	FMT_MTD.1/GP-PR FMT_MTD.1/GP-LC
FPT_FLS.1/GP	No Dependencies	No Dependencies
FPT_RCV.3/GP	AGD_OPE.1	AGD_OPE.1
FCO_NRO.2/GP	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FDP_UIT.1/GP	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) (FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FIA_UID.1/GP	No Dependencies	No Dependencies
FMT_SMF.1/GP	No Dependencies	No Dependencies
FMT_SMR.1/GP	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FTP_ITC.1/GP	No Dependencies	No Dependencies

SFRs	CC Dependencies	Satisfied Dependencies
FMT_MSA.1/GP	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/GP FMT_SMR.1/GP
FMT_MTD.1/GP-PR	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/GP FMT_SMF.1/GP
FDP_ITC.2/GP-ELF	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) (FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path) FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_IFC.2/GP-ELF FTP_ITC.1/GP FPT_TDC.1/GP
FDP_IFC.2/GP-ELF	FDP_IFF.1 Simple security attributes	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FDP_ITC.2/GP-KL	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) (FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path) FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_IFC.2/GP-KL FTP_ITC.1/GP FPT_TDC.1/GP
FDP_IFC.2/GP-KL	FDP_IFF.1 Simple security attributes	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.2/GP-KL FMT_MSA.3/GP
FMT_MTD.1/GP-LC	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/GP FMT_SMF.1/GP
FTP_TRP.1/GP-TF	No Dependencies	No Dependencies
FCS_RNG.1/GP-SCP	No Dependencies	No Dependencies
FCS_CKM.1/GP-SCP	(FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/GP-SCP FCS_CKM.4 (from [PP-JC])

SFRs	CC Dependencies	Satisfied Dependencies
FCS_COP.1/GP-SCP	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/GP-SCP FCS_CKM.4 (from [PP-JC])

7.3.3.2 SARs Dependencies

Table 7-15: SARs Dependencies

SARs	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2

SARs	CC Dependencies	Satisfied Dependencies
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

7.3.4 Rationale for the Security Assurance Requirements

EAL4 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. The targeted EAL4 is augmented with AVA_VAN.5 implementing the resistance requirement against attackers with high attack potential. This evaluation assurance level allows a developer to gain high assurance from positive security engineering based on good practices. The targeted EAL4 represents the best current practical compromise between the level of assurance and resistance to attackers. The level AVA_VAN.5 is only achieved if the vulnerability assessment is based on analysis of low-level hardware design and source code analysis.

7.3.5 AVA_VAN.5 Advanced Methodical Vulnerability Analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for Java Card/GlobalPlatform technology-based products hosting sensitive applications, particularly in payment and identity areas. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1, and AGD_OPE.1. All these assurance requirements are met by EAL4.

7.3.6 ALC_DVS.2 Sufficiency of Security Measures

Development security is concerned with physical, procedural, personnel, and other technical measures that shall be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the sensitivity of the TOE and embedded software, it is necessary to justify the sufficiency of these requirements protecting the integrity and confidentiality of the TOE during development. ALC_DVS.2 has no dependencies.

8 Package ‘Ciphered Load File Data Block (CLFDB)’

8.1 Scope

The Package ‘CLFDB’ is to be considered when the encryption of Load File Data Block is required. This privilege allows an SD Provider to require ciphering the Load File Data Block. The SD who has this privilege will be requested by the OPEN to decrypt the Load File Data Blocks and their associated Executable Load Files.

8.2 SPD

Table 8-1: SPDs of CLFDB Package

Assets	
D.CLFDB-DK	Symmetric key to be used to decrypt Load File Data Blocks. To be protected from unauthorised disclosure and modification. *Application Note*: See [GPCS] section C.1.3.
Threats	
T.CLFDB-DISC	Threat agent: Attacker Adverse action: The attacker discloses a Ciphered Load File Data Block when it is transmitted to the SE for decryption prior to installation. Directly threatened asset(s): All assets are threatened. Note: This threat refines T.COM-EXPLOIT to address the CLFDB.
Organisational Security Policies	
OSP.CLFDB-ENC-PR	The Load File Data Block must be encrypted securely by a trusted SD provider. *Application Note*: See [GPCS] section C.6.

8.3 Objectives

Table 8-2: Objectives of CLFDB Package

Security Objectives for the TOE	
O.CLFDB-DECIPHER	If the SD to be associated with the Executable Load File has the Ciphered Load File Data Block privilege, then the card shall support encryption schemes as defined by GlobalPlatform specifications and the SD shall be able to decipher the Ciphered Load File Data Blocks. *Application Note*: See [GPCS] section C.6.
Security Objectives for the Operational Environment	
OE.CLFDB-ENC-PR	The Load File Data Block shall be encrypted securely by a trusted SD provider. *Application Note*: See [GPCS] section C.6.

8.3.1 Security Objectives Rationale

Table 8-3: Security Objectives Rationale of CLFDB Package

Threats, OSPs	Objectives	Rationale
T.CLFDB-DISC	O.CLFDB-DECIPHER	O.CLFDB-DECIPHER protects the Ciphered Load File Data Block when it is transmitted to the SE for decryption prior to installation.
OSP.CLFDB-ENC-PR	OE.CLFDB-ENC-PR	This OSP is enforced by the security objective for the operational environment of the TOE OE.CLFDB-ENC-PR.

8.4 Security Functional Requirements

FCS_COP.1/GP-CLFDB Cryptographic operation

FCS_COP.1.1/GP-CLFDB The TSF shall perform **Decryption of Ciphered Load File Data Blocks** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- See [GPCS] section C.6.
- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].
- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.

Table 8-4: Algorithms Used to Decrypt CLFDB

Algorithm	Key sizes	Recommended Standards
TDES with CBC mode	112 bits	[ISO 9797-1]
AES with CBC mode with a null ICV	128, 192, or 256 bits	[FIPS 197]

See recommendation 1 from Table 2-1.

8.5 Security Requirements Rationale

Table 8-5: Security Requirements Rationale of CLFDB Package

Security Objectives	SFRs	Rationale
O.CLFDB-DECIPHER	FCS_COP.1/GP-CLFDB	FCS_COP.1/GP-CLFDB specifies the cryptographic operations and algorithms that shall be used to decrypt the Ciphered Load File Data Block when it is received by the SE.

8.6 SFR Dependencies

Table 8-6: SFR Dependencies of CLFDB Package

SFRs	CC Dependencies	Satisfied Dependencies
FCS_COP.1/GP-CLFDB	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2/GP-ELF FCS_CKM.4 (from PP JCP)

9 Package ‘Global Services (GS)’

9.1 Scope

The Package ‘GS’ is to be considered when an Application implements and provides services to other Applications on the card. The Global Services Applications are distinguished by having the Global Service privilege. Examples of such services are Cardholder Verification Method (CVM) services.

9.2 SPD

Table 9-1: SPDs of GS Package

Assets	
D.GS-PARAMETERS	Global Service Parameters are the service family and the service ID within that family. To be protected from unauthorised modification. *Application Note*: As defined in [GPCS] section 8.1.3. This asset is an extension of D.GP_REGISTRY.
Threats	
T.UNAUTHORISED-CARD-MGMT from this PP.	

9.3 Objectives

Table 9-2: Objectives of GS Package

Security Objectives for the TOE
O.CARD-MANAGEMENT from this PP.

9.3.1 Security Objectives Rationale

Table 9-3: Security Objectives Rationale of GS Package

Threats	Objectives	Rationale
T.UNAUTHORISED-CARD-MGMT	O.CARD-MANAGEMENT	O.CARD-MANAGEMENT controls the access to card management functions such as the loading, installation, extradition, or deletion of applets.

9.4 Security Functional Requirements

FDP_ACC.1/GP-GS Subset access control

FDP_ACC.1.1/GP-GS The TSF shall enforce the **GlobalPlatform Services access control policy** on **the following list of subjects, objects and operations:**

- **Subject: S.OPEN, Applications with 'Global Service' privilege, other Applications.**
- **Objects:**
  - **Global Service Privilege**
  - **Service name**
  - **GlobalPlatform Registry**
  - **AID**
- **Operation controlled by the policy:**
  - **Registration of a Global Service with a unique service name**
  - **Deregistration of a Global Service with a unique service name**
  - **Access of a uniquely registered Global Service or a specific Global Services Application.**

FDP_ACF.1/GP-GS Security attribute based access control

FDP_ACF.1.1/GP-GS The TSF shall enforce the **GlobalPlatform Services access control policy** to objects based on the following:

- **Security Attributes:**
  - **Global Service privilege: Assigned or Not assigned**
  - **Service name: Recorded or Not recorded for an on-card entity (as provided in the INSTALL command)**
  - **Service name: Registered or Not registered in the GlobalPlatform Registry**
  - **AID: Associated or Not associated.**

FDP_ACF.1.2/GP-GS The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Registering/Deregistering Global Services:**
  - **S.OPEN is responsible for ensuring the uniqueness of each service name registered by Global Services Applications.**
  - **On receipt of unique service registration or deregistration request, S.OPEN checks that the requesting on-card entity has the 'Global Service' privilege.**
  - **On receipt of unique service registration request, S.OPEN checks that the requested service name is not registered in the GlobalPlatform Registry for another on-card entity.**
  - **On receipt of service deregistration request, S.OPEN checks that the requested service name is registered in GlobalPlatform Registry entry of the requesting on-card entity.**
- **Application Accessing rules to Global Services:**
  - **On receipt of service access request:**
    - **If the request indicates a specific service name without any associated AID, S.OPEN checks 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, S.OPEN checks 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.**
    - **S.OPEN identifies the corresponding Global Services Application.**
    - **S.OPEN obtains the GlobalPlatform Service interface of the corresponding Global Services Application and forwards it to the requesting on-card entity.**
- **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

FDP_ACF.1.3/GP-GS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/GP-GS The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

Application Note: Global Services Applications are described in [GPCS] section 8.1.

FMT_MSA.1/GP-GS Management of security attributes

FMT_MSA.1.1/GP-GS The TSF shall enforce the **GlobalPlatform Services access control policy** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **defined in FDP_ACF.1.1/GP-GS** to the **S.OPEN**.

FMT_MSA.3/GP-GS Security attribute initialization

FMT_MSA.3.1/GP-GS The TSF shall enforce the **GlobalPlatform Services access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/GP-GS The TSF shall allow the **S.OPEN** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMR.1/GP-GS Security roles

FMT_SMR.1.1/GP-GS The TSF shall maintain the roles **S.OPEN, Global Services Application**.

FMT_SMR.1.2/GP-GS The TSF shall be able to associate users with roles.

FMT_SMF.1/GP-GS Specification of Management Functions

FMT_SMF.1.1/GP-GS The TSF shall be capable of performing the following management functions:

- **Management of Global Services Applications (Registering, Deregistering, Accessing)**
- **[assignment: list of management functions to be provided by the TSF].**

Application Note:

Global Services Applications are described in [GPCS] section 8.1.

9.5 Security Requirements Rationale

Table 9-4: Security Requirements Rationale of GS Package

Security Objectives	SFRs	Rationale
O.CARD-MANAGEMENT	FDP_ACC.1/GP-GS, FDP_ACF.1/GP-GS, FMT_MSA.1/GP-GS, FMT_MSA.3/GP-GS, FMT_SMF.1/GP-GS, FMT_SMR.1/GP-GS	• FDP_ACC.1/GP-GS, FDP_ACF.1/GP-GS enforce the GlobalPlatform Services access control policy for managing the registration, deregistration, and access of the Global Service. • FMT_MSA.1/GP-GS and FMT_MSA.3/GP-GS specify security attributes that support management of the Global Service privilege, the service name and AID. • FMT_SMR.1/GP-GS maintains the roles S.OPEN, Global Services Application and their associated Life Cycle states. • FMT_SMF.1/GP-GS enforces the management of Global Services Applications (Registering, Deregistering, Accessing).

9.6 SFR Dependencies

Table 9-5: SFR Dependencies of GS Package

SFRs	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/GP-GS	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/GP-GS
FDP_ACF.1/GP-GS	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/GP-GS FMT_MSA.3/GP-GS
FMT_MSA.1/GP-GS	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/GP-GS FMT_SMF.1/GP-GS FMT_SMR.1/GP-GS
FMT_MSA.3/GP-GS	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/GP-GS FMT_SMR.1/GP-GS
FMT_SMF.1/GP-GS	No Dependencies	No Dependencies
FMT_SMR.1/GP-GS	FIA_UID.1 Timing of identification	FIA_UID.1/GP

10 Package ‘Cardholder Verification Method (CVM)’

10.1 Scope

The CVM Application, if present on the SE, provides a mechanism for a Cardholder Verification Method (CVM), including velocity checking, that may be used by all Applications on the card. In [GPCS] v2.3.1, there is one CVM standardised by GlobalPlatform: the global Personal Identification Number (Global PIN); see [GPCS] section 8.2.

CVM functions are delegated from the OPEN to CVM Applications as Global Services Applications (see [GPCS] Chapter 8).

10.2 SPD

Table 10-1: SPDs of CVM Package

Assets	
D.CVM_PIN	A single global PIN used to authenticate the Cardholder, which can be shared by all the application instances in the card. To be protected from unauthorised modification and disclosure.
D.CVM_MGMT_STATE	The CVM management data include: • CVM value and state (e.g. to determine if the CVM value has been submitted, verified, or blocked) • CVM Retry Limit: The maximum number of presentations of invalid CVM values, until the CVM handler rejects further presentation attempts. • CVM Retry Counter: A counter, used in conjunction with the Retry Limit, to determine when attempts for presenting CVM values shall be rejected. To be protected from unauthorised modification.
Threats	
T.CVM-IMPERSONATE	Threat agent: Attacker Adverse action: An attacker could try to impersonate the Cardholder for disclosing or guessing the PIN stored in the CVM, in order to access the services the SE offers. Directly threatened asset(s): D.CVM_PIN
T.CVM-UPDATE	Threat agent: Attacker Adverse action: An attacker could try executing an application that tries to modify (reset/update) the CVM management data (Retry Limit, retry Counter, CVM value and state). Directly threatened asset(s): D.CVM_MGMT_STATE
T.BRUTE-FORCE-CVM	Threat agent: Attacker Adverse action: APDU commands/API methods could be repeatedly transmitted/invoked to attempt the brute force extraction of secrets such as PINs. Directly threatened asset(s): D.CVM_PIN, D.CVM_MGMT_STATE

10.3 Objectives

Table 10-2: Objectives of CVM Package

Security Objectives for the TOE	
O.GLOBAL-CVM	The TOE shall restrict the modification of the security attributes of the CVM only to defined privileged applications appointed by the Card Manager. Any SD allowed to perform CVM can grant the CVM privilege to an Application.
O.CVM-BLOCK	If the maximum number of attempts has been reached, further Cardholder authentication attempts are blocked. The blocking can be removed by special action of the Card Manager or a privileged user.
O.CVM-MGMT	The TOE shall provide means to securely manage CVM objects. Secure management of CVM objects includes: • Atomic update of PIN code and of the try counter, • No rollback of the number of unsuccessful authentication attempts, • Protection of confidentiality of the PIN value, • Protection of the PIN comparison process against observation.

10.3.1 Security Objectives Rationale

Table 10-3: Security Objectives Rationale of CVM Package

Threats	Objectives	Rationale
T.CVM-IMPERSONATE	O.GLOBAL-CVM, O.CVM-BLOCK, O.CVM-MGMT	O.GLOBAL-CVM restricts the modification of the security attributes of the CVM only to defined privileged applications appointed by the Card Manager. O.CVM-BLOCK blocks the global PIN used to authenticate the Cardholder if the maximum number of attempts has been reached. O.CVM-MGMT securely manages CVM objects.
T.BRUTE-FORCE-CVM	O.CVM-BLOCK, O.CVM-MGMT	O.CVM-BLOCK blocks the global PIN used to authenticate the Cardholder if the maximum number of attempts has been reached. O.CVM-MGMT securely manages CVM objects.
T.CVM-UPDATE	O.CVM-BLOCK, O.CVM-MGMT	

10.4 Security Functional Requirements

FIA_AFL.1/GP-CVM Authentication failure handling

FIA_AFL.1.1/GP-CVM The TSF shall detect when **[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]** unsuccessful authentication attempts occur related to **user authentication using CVM**.

FIA_AFL.1.2/GP-CVM When the defined number of unsuccessful authentication attempts has been **[selection: met, surpassed]**, the TSF shall **[assignment: list of actions]**.

FPR_UNO.1/GP-CVM Unobservability

FPR_UNO.1.1/GP-CVM The TSF shall ensure that **[assignment: list of users and/or subjects]** are unable to observe the operation **comparison** on **Global PIN** by **[assignment: list of protected users and/or subjects]**.

10.5 Security Requirements Rationale

Table 10-4: Security Requirements Rationale of CVM Package

Security Objectives	SFRs	Rationale
O.CVM-BLOCK	FIA_AFL.1.1/GP-CVM	FIA_AFL.1.1/GP-CVM detects the authentication failure attempts related to user authentication using CVM.
O.CVM-MGMT	FIA_AFL.1.1/GP-CVM, FPR_UNO.1/GP-CVM	FPR_UNO.1/GP-CVM ensures that unauthorised users are unable to observe the comparison on Global PIN. FIA_AFL.1.1/GP-CVM detects the authentication failure attempts related to user authentication using CVM.
O.GLOBAL-CVM	FPR_UNO.1/GP-CVM	FPR_UNO.1/GP-CVM ensures that unauthorised users are unable to observe the comparison on Global PIN.

10.6 SFR Dependencies

Table 10-5: SFR Dependencies of CVM Package

SFRs	CC Dependencies	Satisfied Dependencies
FIA_AFL.1.1/GP-CVM	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/GP-GS
FPR_UNO.1/GP-CVM	No Dependencies	No Dependencies

11 Package ‘Delegated Management (DM)’

11.1 Scope

This Package is to be considered if the Supplementary Security Domains have the ‘Delegated Management’ privilege.

The DM privilege allows an Application Provider to manage Card Content with authorisation. Within a sub-hierarchy of SDs starting from the SD with the ‘Authorised Management’ privilege, the descendant SD that has the ‘Token Verification’ privilege (and optionally the ‘Receipt Generation’ privilege) controls such authorisation.

The DM privilege allows an APSD with this privilege to perform:

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

11.2 SPD

Table 11-1: SPDs of DM Package

Assets	
D.TOKEN-VERIFICATION-KEY	The symmetric key or the public asymmetric key to be used for token verification. To be protected from unauthorised modification and disclosure.
D.RECEIPT-GENERATION-KEY	The symmetric key or the private asymmetric key to be used for receipt generation. To be protected from unauthorised modification and disclosure.
D.CONFIRMATION-DATA	The confirmation Data generated by an SD with the Receipt Generation Privilege. To be protected from unauthorised modification. *Application Note*: See [GPCS] section 11.1.6.
Threats	
T.RECEIPT	Threat agent: Attacker Adverse action: The attacker may generate fake receipts in order to hide or falsify completion proofs of card management operations. Directly threatened asset(s): D.RECEIPT-GENERATION-KEY, D.CONFIRMATION-DATA
T.TOKEN	Threat agent: Attacker Adverse action: The attacker may try to impersonate the Card Manager in order to gain access to the card and perform illegitimate card management operations. Directly threatened asset(s): D.TOKEN-VERIFICATION-KEY

Organisational Security Policies	
OSP.TOKEN-GEN	The Token must be generated securely by a trusted entity according to the signature algorithms defined in GlobalPlatform specifications. *Application Note*: See [GPCS] sections B.1, B.2, B.3, B.4, and C.4.
OSP.RECEIPT-VER	The Receipt must be verified securely by a trusted entity according to the methods defined in GlobalPlatform specifications. *Application Note*: See [GPCS] sections B.1, B.2, B.3, B.4, and C.5.

11.3 Objectives

Table 11-2: Objectives of DM Package

Security Objectives for the TOE	
O.RECEIPT	The TOE shall generate non-repudiable receipts of the completion of card management operations. The generation of the receipt shall be performed by an SD with 'Receipt Generation' Privilege.
O.TOKEN	The TOE shall verify tokens during the processing of card management operations. The verification of the token shall be performed by an SD with 'Token Verification' Privilege.
Security Objectives for the Operational Environment	
OE.TOKEN-GEN	The Token shall be generated securely by a trusted entity according to the signature algorithms defined in GlobalPlatform specifications. *Application Note*: See [GPCS] sections B.1, B.2, B.3, B.4, and C.4.
OE.RECEIPT-VER	The Receipt shall be verified securely by a trusted entity according to the methods defined in GlobalPlatform specifications. *Application Note*: See [GPCS] sections B.1, B.2, B.3, B.4, and C.5.

11.3.1 Security Objectives Rationale

Table 11-3: Security Objectives Rationale of DM Package

Threats, OSPs	Objectives	Rationale
T.RECEIPT	O.RECEIPT	O.RECEIPT generates non-repudiable receipts of the completion of card management operations.
T.TOKEN	O.TOKEN	O.TOKEN verifies tokens during the processing of card management operations.
OSP.TOKEN-GEN	OE.TOKEN-GEN	This OSP is enforced by the security objective for the operational environment of the TOE OE.TOKEN-GEN.
OSP.RECEIPT-VER	OE.RECEIPT-VER	This OSP is enforced by the security objective for the operational environment of the TOE OE.RECEIPT-VER.

11.4 Security Functional Requirements

FCO_NRR.1/GP-RECEIPT Selective proof of receipt

FCO_NRR.1.1/GP-RECEIPT The TSF shall be able to generate evidence of receipt for received **card management operation requests** at the request of the **originator**.

FCO_NRR.1.2/GP-RECEIPT The TSF shall be able to relate the **Confirmation Data** of the recipient of the information, and the parameters of **the card management operation request** of the information to which the evidence applies.

FCO_NRR.1.3/GP-RECEIPT The TSF shall provide a capability to verify the evidence of receipt of information to **recipient** given **none**.

Application Note:

The confirmation data are described in [GPCS] section 11.1.6.

The parameters of the card management operation request are described in [GPCS] section C.5.

FCO_NRO.2/GP-TOKEN Enforced proof of origin

FCO_NRO.2.1/GP-TOKEN The TSF shall enforce the generation of evidence of origin for transmitted **[assignment: list of information types]** at all times.

Refinement

The TSF shall be able to generate an evidence of origin at all times for 'ELF with Token Verification' received from the off-card entity (originator of transmitted data) that communicates with the card.

FCO_NRO.2.2/GP-TOKEN The TSF shall be able to relate the **[assignment: list of attributes]** of the originator of the information, and the **[assignment: list of information fields]** of the information to which the evidence applies.

Refinement

The TSF shall be able to load 'ELF with Token Verification' to the card with associated security attributes (token present in the card management operation request) such that the authenticity of transmitted data can be verified.

FCO_NRO.2.3/GP-TOKEN The TSF shall provide a capability to verify the evidence of origin of information to **the off-card entity (recipient of the evidence of origin) requesting that verification** given **at the time the ELF with Token is received**.

Application Note:

The parameters of the card management operation request are described in [GPCS] section C.4.

FCS_COP.1/GP-TOKEN Cryptographic operation

FCS_COP.1.1/GP-TOKEN The TSF shall perform **the verification of the Token signature attached to card management commands** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- The token verification shall meet the annex C.4 'Tokens' and the following sections of [GPCS]:
  - RSA as defined in [GPCS] section B.3.1.1 or B3.2.1
  - ECC as defined in [GPCS] section B.4.3
  - DES as defined in [GPCS] section B.1.2.2
  - AES as defined in [GPCS] section B.2.2.
- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].
- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.

Table 11-4: Algorithms Used to Verify the Token Signature

Algorithm	Key sizes	Recommended Standards
TDES	112 bits	[GPCS]
AES	128, 192, or 256 bits	[GPCS]
RSA	1024 to 4096 bits	[GPCS]
ECC	256, 384, or 512 bits	[GPCS]

See recommendations 1 and 2 from Table 2-1.

FCS_COP.1/GP-RECEIPT Cryptographic operation

FCS_COP.1.1/GP-RECEIPT The TSF shall perform **the generation of the Receipt signature attached to responses to card management commands** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- The generation of the receipt shall meet [GPCS] section C.5, 'Receipts', and the following sections of [GPCS]:
  - RSA as defined in [GPCS] section B.3.1.1 or B3.2.1
  - ECC as defined in [GPCS] section B.4.3
  - DES as defined in [GPCS] section B.1.2.2

- AES as defined in [GPCS] section B.2.2.

- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].
- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.

Table 11-5: Algorithms Used to Generate the Receipt Signature

Algorithm	Key sizes	Recommended Standards
TDES	112 bits	[GPCS]
AES	128, 192, or 256 bits	[GPCS]
RSA	1024 to 4096 bits	[GPCS]
ECC	256, 384, or 512 bits	[GPCS]

See recommendations 1 and 2 from Table 2-1.

11.5 Security Requirements Rationale

Table 11-6: Security Requirements Rationale of DM Package

Security Objectives	SFRs	Rationale
O.RECEIPT	FCO_NRR.1/GP-RECEIPT, FCS_COP.1/GP-RECEIPT	FCO_NRR.1/GP-RECEIPT generates evidence of receipt for received card management operation requests. FCS_COP.1/GP-RECEIPT ensures that the card management command has been successfully processed by computing the Receipt signature.
O.TOKEN	FCO_NRO.2/GP-TOKEN, FCS_COP.1/GP-TOKEN	FCO_NRO.2/GP-TOKEN generates an evidence of origin for 'ELF with Token Verification' received from the off-card entity. FCS_COP.1/GP-TOKEN ensures that the card management command is authorised by verifying the Token signature.

11.6 SFR Dependencies

Table 11-7: SFR Dependencies of DM Package

SFRs	CC Dependencies	Satisfied Dependencies
FCO_NRR.1/GP-RECEIPT	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FCO_NRO.2/GP-TOKEN	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FCS_COP.1/GP-TOKEN	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2/GP-ELF FDP_ITC.2/GP-KL FCS_CKM.4 (from [PP-JC])
FCS_COP.1/GP-RECEIPT	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2/GP-ELF FDP_ITC.2/GP-KL FCS_CKM.4 (from [PP-JC])

12 Package ‘DAP Verification’

12.1 Scope

The Package ‘DAP Verification’ is to be considered if the implementation supports Supplementary Security Domains (APSD), and an AP requires to be loaded onto the SE in an integrity and authenticity protected way. The ‘DAP Verification’ privilege of the APSD provides this service of verification of Load File Data Block signatures on behalf of an AP.

12.2 SPD

Table 12-1: SPDs of DAP Verification Package

Assets	
D.DAP_BLOCK	Authentication data present in the Load File and generated by an off-card entity (an Application Provider or a Verification Authority). The authentication data contains the SD AID and the Load File Data Block Signature of the Load File Data Block Hash. To be protected from unauthorised modification.
D.APSD_DAP_KEYS	Refinement of D.APP_KEYS of [PP-JC]. The APSD cryptographic keys are required for verification of the Load File Block signatures. To be protected from unauthorised disclosure and modification.
Threats	
T.UNAUTHORISED-CARD-MGMT, T.COM-EXPLOIT from this PP.	
T.INSTALL, T.INTEG-APPLI-CODE.LOAD, T.INTEG-APPLI-DATA.LOAD, T.INTEG-APPLI-CODE, and T.INTEG-APPLI-DATA from [PP-JC].	
Organisational Security Policies	
OSP.DAP_BLOCK_GEN	The DAP Block must be generated securely by a trusted entity that verifies the content of the Load File Data Block linked to the hash.

12.3 Objectives

Table 12-2: Objectives of DAP Verification Package

Security Objectives for the TOE	
O.CARD-MANAGEMENT, O.APPLI-AUTH from this PP.	
O.LOAD, O.INSTALL and O.CIPHER from [PP-JC].	
Security Objectives for the Operational Environment	
OE.DAP_BLOCK_GEN	The DAP Block shall be generated securely by a trusted entity that verifies the content of the Load File Data Block linked to the hash.

12.3.1 Security Objectives Rationale

Table 12-3: Security Objectives Rationale of DAP Verification Package

OSPs	Objectives	Rationale
OSP.DAP_BLOCK_GEN	OE.DAP_BLOCK_GEN	This OSP is enforced by the security objective for the operational environment of the TOE OE.DAP_BLOCK_GEN.

12.4 Security Functional Requirements

FCS_COP.1/GP-DAP_SHA Cryptographic operation

FCS_COP.1.1/GP-DAP_SHA The TSF shall perform **computation of a hash value for DAP Verification** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- Refer to the description in [GPCS] section C.3 for more details.
- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].
- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.

Table 12-4: Algorithms Used to Compute the Hash Value for DAP Verification

Algorithm	Key sizes	Recommended Standards
SHA	SHA-1, SHA-256, SHA-384, or SHA-512	[NIST 800-57]

FCS_COP.1/GP-DAP_VER Cryptographic operation

FCS_COP.1.1/GP-DAP_VER The TSF shall perform **verification of the DAP signature attached to Load Files** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- Refer to the description in [GPCS] section C.3 for more details.
- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].
- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.

Table 12-5: Algorithms Used to Verify the DAP Signature

Algorithm	Key sizes	Recommended Standards
TDES	112 bits	[ISO 9797-1]
AES	128, 192, or 256 bits	[NIST 800-38B]
RSA	1024 to 4096 bits	[PKCS#1]
ECC	256, 384, or 512 bits	[ANSI X9.62]

See recommendations 1 and 2 from Table 2-1.

FCO_NRO.2/GP-DAP Enforced proof of origin

FCO_NRO.2.1/GP-DAP The TSF shall enforce the generation of evidence of origin for transmitted **[assignment: list of information types]** at all times.

Refinement

The TSF shall be able to generate an evidence of origin at all times for 'ELF with DAP' received from the off-card entity (originator of transmitted data) that communicates with the card.

FCO_NRO.2.2/GP-DAP The TSF shall be able to relate the **[assignment: list of attributes]** of the originator of the information, and the **[assignment: list of information fields]** of the information to which the evidence applies.

Refinement

The TSF shall be able to load 'ELF with DAP' to the card with associated security attributes (Load File Data Block Signature) such that the integrity and authenticity of transmitted data can be verified.

FCO_NRO.2.3/GP-DAP The TSF shall provide a capability to verify the evidence of origin of information to **the off-card entity (recipient of the evidence of origin) who requested that verification** given **at the time the ELF with DAP is received**.

Application Note:

This SFR addresses the DAP verification as defined in [GPCS] sections 9.2.1, 11.6.2.3, and C.3.

12.5 Security Requirements Rationale

Table 12-6: Security Requirements Rationale of DAP Verification Package

Security Objectives	SFRs	Rationale
O.CARD-MANAGEMENT	FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP	FCS_COP.1/GP-DAP_SHA and FCS_COP.1/GP-DAP_VER ensure that the loaded Executable Application is legitimate by specifying the algorithm to be used in order to verify the DAP signature of the Verification Authority.
O.LOAD	FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP	

Security Objectives	SFRs	Rationale
O.CIPHER	FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP	FCO_NRO.2/GP-DAP generates an evidence of origin for 'ELF with DAP' received from the off-card entity.
O.INSTALL	FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP	
O.APPLI-AUTH	FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP	

12.6 SFR Dependencies

Table 12-7: SFR Dependencies of DAP Verification Package

SFRs	CC Dependencies	Satisfied Dependencies
FCS_COP.1/GP-DAP_SHA	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2/GP-ELF FCS_CKM.4 (from [PP-JC])
FCS_COP.1/GP-DAP_VER	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2/GP-ELF FCS_CKM.4 (from [PP-JC])
FCO_NRO.2/GP-DAP	FIA_UID.1 Timing of identification	FIA_UID.1/GP

13 Package ‘Mandated DAP Verification’

13.1 Scope

The Package ‘Mandated DAP Verification’ is to be considered if the implementation supports Supplementary Security Domains and a Verification Authority requires that all Application code to be loaded onto the SE have to be checked for integrity and authenticity. The ‘Mandated DAP Verification’ privilege of the CASD provides this service on behalf of the VA.

The verification process of DAP is the same as for ‘DAP Verification’ privileges.

In the case of ‘DAP Verification’ privilege, the APSD is responsible for the DAP verification using the APSD keys for DAP. However, in the case of ‘Mandated DAP’ Privilege, the CASD is responsible for the DAP verification using the CASD keys for DAP.

13.2 SPD

Table 13-1: SPDs of MDAP Verification Package

Assets	
D.CASD_DAP_KEYS	Refinement of D.APP_KEYS of [PP-JC]. The CASD cryptographic keys are required for verification of the Load File Data Block signatures. To be protected from unauthorised disclosure and modification.
Threats	
Refer to the list of threats in the Package ‘DAP Verification’.	
Organisational Security Policies	
Refer to the list of OSPs in the Package ‘DAP Verification’.	

13.3 Objectives

Refer to the list of Objectives in the Package ‘DAP Verification’.

13.4 Security Functional Requirements

Refer to the list of SFRs in the Package ‘DAP Verification’.

14 PP-Module Amendment A: Confidential Card Content Management (CCCM)

14.1 Scope

The Confidential Card Content Management (CCCM) PP-Module addresses the security requirements defined in [Amd A]. It covers the following requirements:

- Secure personalisation of APSD by the Controlling Authority with four scenarios:
  - Pull Model (Scenario #1): the APSD keys are generated on-card and retrieved by the AP. The model supports the use of asymmetric and symmetric keys for the transfer of the on-card keys.
  - Push Model (Scenario #2): the APSD keys are generated off-card and 'pushed' to the Application Provider Security Domain protected by asymmetric cryptography. Two different personalisation scenarios are supported, Push Model with and without Application Provider Certificate.
  - Key Agreement Model (Scenario #3): the APSD keys are generated on-card and off-card using the Elliptic curve key agreement scheme described in NIST SP 800-56A [NIST 800-56A] as "(Cofactor) One-Pass Diffie-Hellman, C (1e, 1s, ECC CDH)".
  - Key Agreement Model without Secure Channel (Scenario #4): the APSD keys are generated on-card and off-card using the Elliptic curve key agreement scheme described in [NIST 800-56A] as "(Cofactor) Full Unified Model, C (2e, 2s, ECC CDH)".
- Confidential loading of initial Secure Channel Key Sets.
- Confidential loading of applications by an Application Provider.

14.2 SPD

Table 14-1: SPDs of CCCM PP-Module

Assets	
D.CCCM_KEYS	The on-card generated RGKs with derived keys K_{ENC}, K_{MAC}, and K_{DEK} used to perform Confidential Card Content Management operations. To be protected from unauthorised disclosure and modification.
Threats	
T.COM-EXPLOIT, T.UNAUTHORISED-CARD-MGMT from this PP.	
Organisational Security Policies	
OSP.CCCM	APs not required to share the Secure Channel keys with the Issuer should use one of the CCCM Models.

14.3 Objectives

Table 14-2: Objectives of CCCM PP-Module

Security Objectives for the TOE	
O.CCCM	The TOE shall address the Confidential Card Content Management requirements defined in [Amd A]. These requirements are: • Secure personalisation of APSD by the CA using one of the following scenarios: Pull Model, Push Model, Key Agreement Model, or Key Agreement Model with no Secure Channel • Confidential loading of initial Secure Channel Key Sets • Confidential loading of applications by an AP

14.3.1 Security Objectives Rationale

Table 14-3: Security Objectives Rationale of CCCM PP-Module

Threats, OSPs	Objectives	Rationale
T.COM-EXPLOIT	O.CCCM	O.CCCM requires secure personalisation and confidential loading of secret keys and applications.
T.UNAUTHORISED-CARD-MGMT		
OSP.CCCM		

14.4 Security Functional Requirements

FCS_CKM.1/GP-CCCM Cryptographic key generation

FCS_CKM.1.1/GP-CCCM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

This SFR addresses the on-card generation of RGK under the Pull Mode (see [Amd A] section 3.2.1). This key is used on-card and off-card to derive the three APSD Secure Channel keys.

FCS_COP.1/GP-CCCM Cryptographic operation

FCS_COP.1.1/GP-CCCM The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

- The ST writer may define one FCS_COP.1/GP-CCCM for all the cryptographic operations involved in the implementation of personalisation models or one per operation or Model.
- All personalisation models may not be implemented on the same SE. Therefore, the ST writer should select (from the table below) only the cryptographic operations related to the scenario(s) implemented by the SE.
- The personalisation models may all be enabled concurrently on the same SE, except for the symmetric and asymmetric variants of the Pull Mode which are mutually exclusive.
- In case the signature by the CASD of the client Application payload as defined in [Amd A] section 5.3 is supported, the last operation from Table 14-4 should be selected.
- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].

Table 14-4: Cryptographic Operations Involved in Implementation of Personalisation Models

Personalisation Models	Operation	Algorithm	Length	Recommended Standards
Pull Model (Asymmetric and Symmetric Key Modes)	Derivation of the three APSD Secure Channel keys (K_{ENC}, K_{MAC}, and K_{DEK}) from the on-card generated key (RGK)	TDES or AES	112 bits for TDES or 128, 192, 256 bits for AES	[GPCS] section B.1 for TDES [GPCS] section B.2 for AES
Pull Model (Asymmetric Key Mode)	Verification of the AP certificate by the CASD	RSA	1024 to 4096 bits	[GPCS] section B.3
Pull Model (Asymmetric Key Mode)	Encryption of the RGK by the AP Public Key	RSA	1024 to 4096 bits	[GPCS] section B.3
Pull Model (Asymmetric Key Mode)	Signature of the RGS with the CASD Private Key	RSA	1024 to 4096 bits	[GPCS] section B.3
Pull Model (Symmetric Key Mode)	Decryption of the AP Secret Encryption Key using the CASD Symmetric Encryption Key	TDES or AES	112 bits for TDES or 128, 192, 256 bits for AES	[GPCS] section B.1 for TDES [GPCS] section B.2 for AES
Pull Model (Symmetric Key Mode)	Signature Verification of the AP Secret Encryption Key by the CASD Symmetric Signature Key	TDES or AES	112 bits for TDES or 128, 192, 256 bits for AES	[GPCS] section B.1 for TDES [GPCS] section B.2 for AES
Pull Model (Symmetric Key Mode)	Encryption of the RGK by the AP Secret Encryption Key	TDES or AES	112 bits for TDES or 128, 192, 256 bits for AES	[GPCS] section B.1 for TDES [GPCS] section B.2 for AES

Personalisation Models	Operation	Algorithm	Length	Recommended Standards
Pull Model (Symmetric Key Mode)	Signature of the RGK with the CASD Signature Key	TDES or AES	112 bits for TDES or 128, 192, 256 bits for AES	[GPCS] section B.1 for TDES [GPCS] section B.2 for AES
Push Model with AP certificate	Verification of the AP Certificate by the CASD using its public key	RSA	1024 to 4096 bits	[GPCS] section B.3
Push Model with AP certificate	Signature verification of the APSD keys by the APSD using the public key extracted from the AP certificate	RSA	1024 to 4096 bits	[GPCS] section B.3
Push Model with or without AP certificate	Decryption of the APSD keys using the CASD private key	RSA	1024 to 4096 bits	[GPCS] section B.3
Push Model without AP certificate	Decryption of the APSD keys using the temporary APSD Secure Channel keys	RSA	1024 to 4096 bits	[GPCS] section B.3
Push Model without AP certificate	Signature verification of the APSD keys by the temporary APSD Secure Channel keys	RSA	1024 to 4096 bits	[GPCS] section B.3
Key agreement Model	Key Agreement (Cofactor) One-Pass Diffie-Hellman, C(1e, 1s, ECC CDH) scheme	ECC	256, 384, 512, or 521 bits	[NIST 800-56A] and [GPCS] section B.4
Key agreement Model	Signature generation of the CASD certificate	ECDSA	256, 384, 512, or 521 bits	[GPCS] section B.4
All	Signature by the CASD of the client Application payload	ECDSA	256, 384, 512, or 521 bits	[RFC 5758]

See recommendations 1 to 3 from Table 2-1.

FDP_IFC.2/GP-CCCM Complete information flow control

FDP_IFC.2.1/GP-CCCM The TSF shall enforce the **Confidential Personalisation of Secure Channel Keys information flow control SFP** on:

- **Subjects: S.SD, S.CAD, S.OPEN, Application**

- **Information: GlobalPlatform APDU commands INITIALIZE SECURITY (Scenario #4), STORE DATA and PUT KEY, GlobalPlatform APIs for Confidential Personalisation (Personalisation and Authority interfaces)**

  and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/GP-CCCM The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Application Note:

- PUT KEY and STORE DATA commands are described in sections 11.8 and 11.11 respectively.
- INITIALIZE SECURITY command used under the scenario #4 (Key Agreement Model with no Secure Channel) is described in [Amd A] section 3.5.5.
- APIs for confidential personalisation are described in [Amd A] section 4.
- The subject S.SD can be the ISD, an APSD, or the CASD.

FDP_IFF.1/GP-CCCM Complete information flow control

FDP_IFF.1.1/GP-CCCM The TSF shall enforce the **Confidential Personalisation of Secure Channel Keys information flow control SFP** based on the following types of subject and information security attributes:

- **Security Attributes: Status of CASD (installed, personalised, associated with ISD)**
- **[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]**

FDP_IFF.1.2/GP-CCCM The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **There is a single instance of CASD that is installed, personalised, and associated with ISD.**
- **The confidential personalisation of APSD is performed using one of the scenarios #1, #2A, #2B, #3, or #4, as defined in [Amd A].**
- **The confidential personalisation of APSD is performed by using the CASD cryptographic functions.**
- **[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]**

FDP_IFF.1.3/GP-CCCM The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/GP-CCCM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/GP-CCCM The TSF shall explicitly deny an information flow based on the following rules:

- **S.SD fails to unwrap INITIALIZE SECURITY, STORE DATA, or PUT KEY.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**

- **CASD is not installed.**
- **CASD is not personalised to enable the personalisation of APSD.**
- **CASD is not associated with the ISD.**
- **[assignment: rules, based on security attributes, that explicitly deny information flows]**

Application Note:

Personalisation Models and scenarios are described in [Amd A] section 3.2.

- For the Pull Model (Scenario #1), see [Amd A] section 3.2.1.
- For the Push Model (Scenario #2), see [Amd A] section 3.2.2.
- For the Key Agreement Model (Scenario #3), see [Amd A] section 3.2.3.
- For the Key Agreement with no Secure Channel (Scenario #4), see [Amd A] section 3.2.4.

FMT_MSA.1/GP-CCCM Management of security attributes

FMT_MSA.1.1/GP-CCCM The TSF shall enforce the **Confidential Personalisation of Secure Channel Keys information flow control SFP** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **defined in FDP_IFF.1.1/GP-CCCM** to the **[assignment: the authorised identified roles]**.

FMT_MSA.3/GP-CCCM Security attribute initialization

FMT_MSA.3.1/GP-CCCM The TSF shall enforce the **Confidential Personalisation of Secure Channel Keys information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/GP-CCCM The TSF shall allow the **[assignment: the authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

FTP_ITC.1/GP-CCCM Inter-TSF trusted channel

FTP_ITC.1.1/GP-CCCM The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/GP-CCCM The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/GP-CCCM The TSF shall initiate communication via the trusted channel for:

- **Confidential personalisation of Secure Channel Keys (setup of initial keys and update of existing keys) as defined in [Amd A]**
- **Secure personalisation of APSD by the CA through the CASD as defined in [Amd A]**
- **Confidential loading of applications by an AP as defined in [Amd A]**

- **[assignment: list of functions for which a trusted channel is required].**

Application Note:

Confidential personalisation of Secure Channel Keys (setup of initial keys and update of existing keys) is defined in [Amd A] section 3.2 and [GPCS] sections 11.8 and 11.11.

The trusted channel is not required for the Key Agreement Model (Scenario #4). In this model, Security Domain keys are generated on-card and off-card using the Elliptic curve key agreement scheme described in [NIST 800-56A] as "(Cofactor) Full Unified Model, C (2e, 2s, ECC CDH)".

14.5 Security Requirements Rationale

Table 14-5: Security Requirements Rationale of CCCM PP-Module

Security Objectives	SFRs	Rationale
O.CCCM	FCS_CKM.1/GP-CCCM, FCS_COP.1/GP-CCCM, FDP_IFF.1/GP-CCCM, FMT_MSA.1/GP-CCCM, FMT_MSA.3/GP-CCCM, FDP_IFC.2/GP-CCCM, FTP_ITC.1/GP-CCCM	FCS_CKM.1/GP-CCCM addresses the on-card generation of RGK under the Pull Mode. FCS_COP.1/GP-CCCM specifies the cryptographic algorithms used to personalise the APSD. FDP_IFC.2/GP-CCCM and FDP_IFF.1/GP-CCCM enforce the information flow control policy for managing, authenticating, and protecting the Confidential Card management commands and responses between off-card and on-card entities. FMT_MSA.1/GP-CCCM and FMT_MSA.3/GP-CCCM specify security attributes protecting the confidentiality of card management commands, and enforcing the Confidential Personalisation of Secure Channel Keys. FTP_ITC.1/GP-CCCM requires a trusted channel for the confidential Personalisation of Secure Channel Keys, APSD, and the confidential loading of applications by an Application Provider as defined in [Amd A].

14.6 SFR Dependencies

Table 14-6: SFR Dependencies of CCCM PP-Module

SFRs	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/GP-CCCM	(FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/GP-CCCM FCS_CKM.4 (from [PP-JC])
FCS_COP.1/GP-CCCM	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/GP-CCCM FCS_CKM.4 (from [PP-JC])
FDP_IFC.2/GP-CCCM	FDP_IFF.1 Simple security attributes	FDP_IFF.1/GP-CCCM
FDP_IFF.1/GP-CCCM	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.2/GP-CCCM FMT_MSA.3/GP
FTP_ITC.1/GP-CCCM	No Dependencies	No Dependencies
FMT_MSA.1/GP-CCCM	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/GP-CCCM FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP-CCCM	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/GP-CCCM FMT_SMR.1/GP

14.7 Consistency Rationale

The CCCM PP-Module is consistent with the core SE PP and packages:

- The TOE type defined in the PP-Module is based on the TOE type defined in the core PP and packages.
- There are additional objectives for the TOE, which do not contradict or invalidate the objectives of the core PP and packages.
- There are additional SFRs, which do not contradict or invalidate the SFRs of the core PP and packages.

15 PP-Module Amendment C: Contactless Services (CTL)

15.1 TOE Type

The PP-Module for [Amd C] extends the TOE of the core PP with Contactless Services. These services concern the following main entities:

- The Contactless Registry Service (CRS) which is an extension of the OPEN providing:
  - The Contactless Registry, an extension of the GlobalPlatform Registry,
  - The CRS API, an extension of the GlobalPlatform API,
  - Services for managing and accessing the Contactless Registry parameters,
  - Contactless protocol management,
  - Access control on Communication Interfaces,
  - Application selection rules on the contactless interface,
  - Contactless privileges.
- The Contactless Registry Event Listener (CREL) Application which is notified of the changes occurring to one or more Contactless Applications.

The CRS Application is an optional component designed for the management of Contactless Applications by the end user which is not part of the TOE.

15.2 SPD

Table 15-1: SPDs of CTL PP-Module

Assets	
D.CTL_REGISTRY	Contactless Registry contains contactless-related data such as: • Application AID • Application Life Cycle State • Contactless Activation State • Contactless Protocol Type State • Update Counters • CREL Application AID List To be protected from unauthorised modification. *Application Note*: This asset is an extension of D.GP_REGISTRY. See [Amd C] Table 3-9 for the data.
D.CTL_PRO	Contains the contactless Protocol Parameters. To be protected from unauthorised modification. *Application Note*: This asset is an extension of D.GP_REGISTRY.

Threats	
T.CTL-REGISTRY-OVERWRITE	Threat agent: Attacker Adverse action: The attacker attempts to modify the contents of the Contactless Registry in order to: • Set an application in an unauthorised state (e.g. ACTIVATE a NON_ACTIVATABLE application) • Reset the counter Directly threatened asset(s): D.CTL_REGISTRY, D.CTL_PRO
T.COUNTERS-FREEZE	Threat agent: Attacker Adverse action: The attacker attempts to prevent the counter increment in order to have an operation performed twice as the off-card entity believes no transition has taken place. Directly threatened asset(s): D.CTL_REGISTRY, D.CTL_PRO
T.CTL-AUTH-FORGE	Threat agent: Attacker Adverse action: The attacker attempts to use the STORE DATA command in order to modify the blacklist of tokens and reuse a blacklisted CCM token. The attacker may also use this command to make CRS visible on the CTL interface whereas CRS personalisation is not complete, in order to perform unauthorised transactions. Directly threatened asset(s): D.CTL_REGISTRY, D.CTL_PRO
T.CRS-BYPASS	Threat agent: Attacker Adverse action: The attacker grants the CRS privileges to an unauthorised application in order to perform unauthorised state transitions (e.g. set a NON-ACTIVATABLE application to ACTIVATED or DEACTIVATED, or make it visible). Directly threatened asset(s): D.CTL_REGISTRY, D.CTL_PRO

15.3 Objectives

Table 15-2: Objectives of CTL PP-Module

Security Objectives for the TOE	
O.CTL_REGISTRY	The CRS shall ensure that only authorised changes in the Contactless Registry are performed. The SET STATUS command shall only impact CRS-registered applications and shall not perform unauthorised state transitions. The Contactless Registry shall be integrity protected like other data in the OPEN. The CRS shall ensure that the activation state of CRS-registered applications reflects the Contactless Registry content.
O.CTL_SC	The CRS shall ensure that the STORE DATA command to modify blacklists of CCM tokens or to change the CRS visibility state on the CTL interface comes through a Secure Channel with at least level “AUTHENTICATED”.
O.CRS_PRIVILEGES	The CRS shall securely manage the assignment of the ‘Contactless Activation’ Privilege and the ‘Global Registry’ Privilege.
O.CRS_COUNTERS	The CRS shall ensure that the Update Counters are protected for integrity and increased by one at each completed operation or sequence of operations.

15.3.1 Security Objectives Rationale

Table 15-3: Security Objectives Rationale of CTL PP-Module

Threats	Objectives	Rationale
T.CTL-REGISTRY-OVERWRITE	O.CTL_REGISTRY	O.CTL_REGISTRY ensures that only authorised changes in the Contactless Registry are performed.
T.CTL-AUTH-FORGE	O.CTL_SC	O.CTL_SC ensures that the modification of blacklists of CCM tokens or the CRS visibility state on the CTL interface comes through a Secure Channel.
T.CRS-BYPASS	O.CRS_PRIVILEGES	O.CRS_PRIVILEGES manages the assignment of the 'Contactless Activation' Privilege and the 'Global Registry' Privilege.
T.COUNTERS-FREEZE	O.CRS_COUNTERS	O.CRS_COUNTERS ensures that the Update Counters are protected for integrity and increased by one at each completed operation or sequence of operations.

15.4 Security Functional Requirements

FDP_ACC.1/GP-CTL Subset access control

FDP_ACC.1.1/GP-CTL The TSF shall enforce the **CTL Registry access control policy** on **the following list of subjects, objects and operations:**

- **Subjects: CRS/OPEN, CREL Application(s), Applications**
- **Objects: Contactless Registry**
- **Operation controlled by the policy: APDU commands and CTL API methods**

Application Note:

APDU commands are described in [Amd C] section 3.11.

CTL API methods are described in [Amd C] Annex A.

FDP_ACF.1/GP-CTL Security attribute based access control

FDP_ACF.1.1/GP-CTL The TSF shall enforce the **CTL Registry access control policy** to objects based on the following:

- **Security Attributes: Contactless Activation State (ACTIVATED, DEACTIVATED, NON_ACTIVATABLE), Contactless privilege, Communication Interface Availability (Enabled, Disabled), System Install parameter.**

FDP_ACF.1.2/GP-CTL The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Rules to be applied on the registration of a CTL Application**
    - **If the TOE contains at least one application for contactless communication, then this application has to get the Contactless Activation Privilege. This rule is enforced by the CRS/OPEN.**
    - **An Application in the NON_ACTIVATABLE state is implicitly DEACTIVATED and cannot be ACTIVATED. Any attempt to activate an Application that is currently in the NON_ACTIVATABLE state shall fail.**
    - **No application shall be capable of transitioning itself into the ACTIVATED state, except the application having the Contactless Self-Activation Privilege.**
    - **Privacy-sensitive applications and non-privacy-sensitive applications cannot be activated and operated at the same time (Privacy Sensitive Applications are identified by a new System Install parameter).**
    - **When an Application transitions from the INSTALLED state to the SELECTABLE state, the CRS/OPEN may attempt to activate the Application. However, this attempt shall fail if the activation of the Application conflicts with other currently activated Applications, or if the Application is in the NON_ACTIVATABLE state.**
    - **When an Application is transitioned to the LOCKED state, it cannot be activated again until the Application gets unlocked.**
- **When a power loss occurs, and not all Applications have been notified of the most recent Registry modification, the following rule applies:**
    - **If no transaction was open at the time of the power loss, notifications for the most recent registry modification are issued again for all Applications upon the next card reset.**
    - **If a transaction was open at the time of the power loss, previous modifications to the Registry are rolled back and the issuance of the notifications is not restarted.**
- **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]**

FDP_ACF.1.3/GP-CTL The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/GP-CTL The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].**

Application Note:

The ST writer may complete the FDP_ACF.1/GP-CTL rules. Refer to the following sections from [Amd C] for additional details:

- Rules defined by [Amd C] section 2.3 for:
  - Populating contactless registry parameters during Application installation ([Amd C] section 2.3.1)
  - Populating contactless registry parameters during Application personalisation ([Amd C] section 2.3.1)
  - Removing contactless registry parameters during Application deletion ([Amd C] section 2.3.1)
  - Activation, deactivation, or change of priority of Contactless Applications (including conflict resolution) ([Amd C] section 2.3.2)
- Rules to be applied to the Head Application as defined in [Amd C] section 3.7.2
- Rules to be applied to Member Application as defined in [Amd C] section 3.7.3
- Rules to be applied when joining or leaving an Application Group as defined in [Amd C] section 3.7.4
- Rules to be applied when creating a Group Authorisation List or adding AIDs to an existing one as defined in [Amd C] section 3.7.5
- Rules to be applied when removing one or more AIDs from the Group Authorisation List as defined in [Amd C] section 3.7.6
- Rules defined in [Amd C] section 3.8 for registering CREL Application, adding to or removing from the CREL List
- Rules defined in [Amd C] section 3.10 for notifying CREL Application(s) and Applications
- Rules to be applied to the Application Update Counter and the Global Update Counter maintained by the CRS as defined in [Amd C] section 3.11.2.3
- Rules for managing the access control on the Contactless Communication Interface as defined in [Amd C] sections 5 and 8.4
- Rules for managing the Contactless privileges as defined in [Amd C] section 7.

FDP_ROL.1/GP-CTL Basic rollback

FDP_ROL.1.1/GP-CL The TSF shall enforce **CTL Registry access control policy** to permit the rollback of the **previous modifications** on the **Contactless registry**.

FDP_ROL.1.2/GP-CL The TSF shall permit operations to be rolled back within the **boundary limit: until the previous modifications to the Registry have been removed from the Registry.**

Application Note: Refer to [Amd C] section 3.10.1 for more details.

FMT_MSA.1/GP-CTL Management of security attributes

FMT_MSA.1.1/GP-CTL The TSF shall enforce the **CTL Registry access control policy** to restrict the ability to **modify** the security attributes **defined in FDP_ACF.1.1/GP-CL** to the **CRS/OPEN.**

FMT_MSA.3/GP-CTL Security attribute initialization

FMT_MSA.3.1/GP-CTL The TSF shall enforce the **CTL Registry access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/GP-CTL The TSF shall allow the **CRS/OPEN** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMR.1/GP-CTL Security roles

FMT_SMR.1.1/GP-CTL The TSF shall maintain the roles **CRS/OPEN and CREL Application(s)**.

FMT_SMR.1.2/GP-CTL The TSF shall be able to associate users with roles.

FMT_SMF.1/GP-CTL Specification of Management Functions

FMT_SMF.1.1/GP-CTL The TSF shall be capable of performing the following management functions:

- **Management of access to contactless registry parameters,**
- **Management of contactless applications,**
- **Management of contactless protocols,**
- **Management of contactless communication interfaces,**
- **Management of contactless privileges,**
- **[assignment: list of management functions to be provided by the TSF]**

FTP_ITC.1/GP-CTL Inter-TSF trusted channel

FTP_ITC.1.1/GP-CTL The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/GP-CTL The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/GP-CTL The TSF shall initiate communication via the trusted channel for **STORE DATA command.**

15.5 Security Requirements Rationale

Table 15-4: Security Requirements Rationale of CTL PP-Module

Security Objectives	SFRs	Rationale
O.CTL_REGISTRY	FDP_ACC.1/GP-CTL, FDP_ACF.1/GP-CTL, FDP_ROL.1/GP-CTL, FMT_MSA.1/GP-CTL, FMT_MSA.3/GP-CTL, FMT_SMR.1/GP-CTL, FMT_SMF.1/GP-CTL	FDP_ACC.1/GP-CTL and FDP_ACF.1/GP-CTL enforce the CTL Registry access control policy for managing of contactless registry parameters, applications, protocols, interfaces, and privileges. FDP_ROL.1/GP-CTL permits the rollback of the previous modifications on the Contactless registry. FMT_MSA.1/GP-CTL and FMT_MSA.3/GP-CTL specify the security attributes that support management of the contactless registry parameters, applications, protocols, interfaces, and privileges. FMT_SMR.1/GP-CTL maintains the roles CRS/OPEN and CREL Application(s) and their associated Life Cycle states. FMT_SMF.1/GP-CTL enforces the management of the contactless registry parameters, applications, protocols, interfaces and privileges.
O.CRS_COUNTERS	FDP_ACC.1/GP-CTL, FDP_ACF.1/GP-CTL, FDP_ROL.1/GP-CTL, FMT_MSA.1/GP-CTL, FMT_MSA.3/GP-CTL, FMT_SMR.1/GP-CTL, FMT_SMF.1/GP-CTL	
O.CRS_PRIVILEGES	FDP_ACC.1/GP-CTL, FDP_ACF.1/GP-CTL, FDP_ROL.1/GP-CTL, FMT_MSA.1/GP-CTL, FMT_MSA.3/GP-CTL, FMT_SMR.1/GP-CTL, FMT_SMF.1/GP-CTL	
O.CTL_SC	FTP_ITC.1/GP-CTL	FTP_ITC.1/GP-CTL requires a trusted channel for the STORE DATA command used to modify blacklists of CCM tokens or to change the CRS visibility state on the CTL interface.

15.6 SFR Dependencies

Table 15-5: SFR Dependencies of CTL PP-Module

SFRs	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/GP-CTL	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/GP-CTL
FDP_ACF.1/GP-CTL	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/GP-CTL FMT_MSA.3/GP-CTL
FDP_ROL.1/GP-CTL	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control)	FDP_ACC.1/GP-CTL
FMT_MSA.1/GP-CTL	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/GP-CTL FMT_SMR.1/GP-CTL FMT_SMF.1/GP-CTL

SFRs	CC Dependencies	Satisfied Dependencies
FMT_MSA.3/GP-CTL	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/GP-CTL FMT_SMR.1/GP-CTL
FMT_SMR.1/GP-CTL	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FMT_SMF.1/GP-CTL	No Dependencies	No Dependencies
FTP_ITC.1/GP-CTL	No Dependencies	No Dependencies

15.7 Consistency Rationale

The Contactless Services PP-Module is consistent with the core PP and packages:

- The TOE type defined in the PP-Module is based on the TOE type defined in the core PP and packages.
- There are additional threats in the PP-Module, and there is no new assumption, which means that the PP-Module does not weaken the core PP and packages.
- There are additional objectives for the TOE, which do not contradict or invalidate the objectives of the core PP and packages.
- There are additional SFRs, which do not contradict or invalidate the SFRs of the core PP and packages.

16 PP-Module Amendment H: Executable Load File Upgrade (ELFU)

16.1 Scope

This PP-Module extends the TOE of the core PP with the Executable Load File (ELF) Upgrade as defined in [Amd H].

An ELF may be shared and used by several Service Providers (e.g. VMPA, which may be instantiated by different banks). Hence, updating an ELF is not only (or not at all) the business of a single Service Provider, but is rather the business of the ELF provider (e.g. Visa in the case of VMPA).

[Amd H] focuses on SE implementing the Java Card Specifications. In particular, it shall be understood that:

- An Executable Load File is a Java Card package.
- An Executable Module is a Java Card Applet class.
- An Application is a Java Card Applet instance.

Each of these will be identified by an AID (Application Identifier).

16.2 SPD

Table 16-1: SPDs of ELFU PP-Module

Assets	
D.OLD_ELF	The ELF being upgraded. It is referred to as the “old ELF version”. To be protected from unauthorised modification.
D.NEW_ELF	The ELF upgrading the old ELF version. It is referred to as the “new ELF version”. To be protected from unauthorised modification.
D.ELF_AID	The ELF AIDs defined in the old and new ELF versions. To be protected from unauthorised modification.
D.ELF_SESSION_ST	The ELF Upgrade Session Status as described in [Amd H] Table 4-8. To be protected from unauthorised modification.
D.ELF_APP_INS	The application instances. To be protected from unauthorised modification and disclosure.
D.ELF_RG_DATA	The registry data including any persistent on-card information related to the application instance which would not be stored or modified by the application instance. To be protected from unauthorised modification.
Threats	
T.ELF-UNAUTHORISED	Threat agent: Attacker Adverse action: An attacker tries to load an ELF without authorisation. Directly threatened asset(s): D.OLD_ELF, D.NEW_ELF, D.ELF_AID

T.ELF-VERSION	Threat agent: Attacker Adverse action: An attacker tries to modify the application version in order to prevent the loading of a new ELF. Directly threatened asset(s): D.OLD_ELF, D.NEW_ELF, D.ELF_AID
T.ELF-DATA-ACCESS	Threat agent: Attacker Adverse action: An attacker tries to access confidential application instance data. Directly threatened asset(s): D.ELF_APP_INS
T.ELF-DATA-INTEGRITY	Threat agent: Attacker Adverse action: An attacker tries to change application instance data. Directly threatened asset(s): D.ELF_APP_INS
T.ELF-SESSION	Threat agent: Attacker Adverse action: An attacker tries to perturb the Session Status to recognize an incomplete upgrade as being complete. Directly threatened asset(s): D.ELF_SESSION_ST
T.ELF-ILL-COMMAND	Threat agent: Attacker Adverse action: An attacker tries to execute forbidden commands during the ELF upgrade session. Directly threatened asset(s): All ELFU PP-Module assets are threatened.
T.ELF-RES-DATA	Threat agent: Attacker Adverse action: An attacker tries to reallocate TOE resources from an user or process to another for gaining unauthorised access to ELF data. Directly threatened asset(s): All ELFU PP-Module assets are threatened.
Organisational Security Policies	
OSP.ELF_DELE_OP	The TOE shall provide the possibility to perform the deletion operation of the Application instances and ELF(s) in one transaction, so that either a full operation or no operation can occur (atomic and irreversible operation).

16.3 Objectives

Table 16-2: Objectives of ELFU PP-Module

Security Objectives for the TOE	
O.ELF_AUTHORISED	Only authorised entities shall be able to load ELFs.
O.ELF_INTEGRITY	The ELF integrity shall be preserved during the loading process – (confidentiality maintained if required).
O.ELF_APP_DATA	The application instance data shall be securely stored when saved. The OPEN shall maintain the integrity & consistency of Registry data.
O.ELF_SESSION	The session status shall be consistent throughout the upgrade process. Forbidden commands shall be rejected during the upgrade process.
O.ELF_DELE_IRR	The TOE must be able to provide an atomic and irreversible deletion operation of the Application instances and ELF(s).

Security Objectives for the TOE	
O.ELF_DATA_PRO	The TOE must ensure that any ELF information contained in a protected resource is not inappropriately disclosed when the resource is reallocated.

16.3.1 Security Objectives Rationale

Table 16-3: Security Objectives Rationale of ELFU PP-Module

Threats, OSPs	Objectives	Rationale
T.ELF-UNAUTHORISED	O.ELF_AUTHORISED, O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH	O.ELF_AUTHORISED ensures that only authorised entities are able to load ELFs. O.CARD-MANAGEMENT controls the access to card management functions such as the loading, installation, extradition, or deletion of applets. O.DOMAIN-RIGHTS restricts the use of an AP security domain key set and therewith the management of applications to the affected SD and to the AP owning the key set. O.COMM-AUTH prevents unauthorised users from initiating a malicious card management operation.
T.ELF-VERSION	O.ELF_INTEGRITY, O.COMM-CONFIDENTIALITY, O.COMM-INTEGRITY	O.ELF_INTEGRITY preserves the ELF integrity and confidentiality (if required) during the loading process. O.COMM-CONFIDENTIALITY prevents disclosure of encrypted data transiting to the card. O.COMM-INTEGRITY protects the integrity of the card management data while it is in transit to the card.
T.ELF-DATA-ACCESS	O.ELF_APP_DATA	O.ELF_APP_DATA maintains the integrity & consistency of Registry data.
T.ELF-DATA-INTEGRITY	O.ELF_APP_DATA	O.ELF_APP_DATA maintains the integrity & consistency of Registry data.
T.ELF-SESSION	O.ELF_SESSION	O.ELF_SESSION ensures that the upgrade process is performed securely.
T.ELF-ILL-COMMAND	O.ELF_SESSION	O.ELF_SESSION ensures that the upgrade process is performed securely.
T.ELF-RES-DATA	O.ELF_DATA_PRO	O.ELF_DATA_PRO protects ELF information when the resource is reallocated.

Threats, OSPs	Objectives	Rationale
OSP.ELF_DELE_OP	O.ELF_DELE_IRR	O.ELF_DELE_IRR provides an atomic and irreversible deletion operation of the Application instances and ELF(s).

16.4 Security Functional Requirements

FDP_ACC.1/GP-ELFU Subset access control

FDP_ACC.1.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** on **the following list of subjects, objects and operations:**

- **Subjects: S.OPEN, ELF Provider, S.SD**
- **Objects: Application instance data, ELF, ELF Registry data, ELF session data**
- **Operation controlled by the policy: APDUs 'MANAGE ELF UPGRADE', INSTALL [for load] and LOAD, and Upgrade API methods.**

Application Note:

The APDU 'MANAGE ELF UPGRADE' is defined in [Amd H] section 4.1.

The INSTALL [for load], LOAD commands, and Upgrade API methods are defined in [Amd H] Annex A.

FDP_ACF.1/GP-ELFU Security attribute based access control

FDP_ACF.1.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** to objects based on the following:

- **Security Attributes: AIDs, ELF session status, ELF versions (old or new).**

FDP_ACF.1.2/GP-ELFU The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Only a single ELF Upgrade Session is processed at a time. No new ELF Upgrade Session may be started until the previous one (if any) has been completed or aborted.**
- **The MANAGE ELF UPGRADE [start] command is rejected with an error and the ELF Upgrade Process is aborted if any of the conditions defined in [Amd H] are satisfied.**
- **S.OPEN allows an ELF upgrade session to be initiated if no other ELF upgrade session is running.**
- **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

FDP_ACF.1.3/GP-ELFU The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/GP-ELFU The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].**

Application Note:

AIDs, ELF session status are given in [Amd H] Table 4-8.

Rules to be applied when starting the Upgrade session are described in [Amd H] section 3.2.1.

Rules to be applied during the Saving phase are described in [Amd H] section 3.2.2.

Rules to be applied during the Loading phase are described in [Amd H] section 3.2.3.

Rules to be applied during the Restore phase are described in [Amd H] section 3.2.4.

Card Content Management Operations described in [Amd H] section 3.4 shall always be rejected during an ELF Upgrade Session.

FDP_ROL.1/GP-ELFU Basic rollback

FDP_ROL.1.1/GP-ELFU The TSF shall enforce **ELF Upgrade Access Control Policy** to permit the rollback of the **deletion** on the **Application instances and ELF(s)**.

FDP_ROL.1.2/GP-ELFU The TSF shall permit operations to be rolled back within the **boundary limit:**

- **If the deletion of the application instances and ELF(s) (atomic and irreversible operation) was started and then interrupted and/or disturbed by for example unexpected power-down, it shall automatically restart and complete at next power-up.**
- **If the interruption occurred during the Deletion Sequence and the latter did not complete automatically (i.e. the irreversible deletion operation did not start already), the Deletion Sequence shall restart.**

FMT_MSA.1/GP-ELFU Management of security attributes

FMT_MSA.1.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** to restrict the ability to **set and maintain** the security attributes **defined in FDP_ACF.1.1/GP-ELFU** to the **S.OPEN.**

FMT_MSA.3/GP-ELFU Security attribute initialization

FMT_MSA.3.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/GP-ELFU The TSF shall allow the **S.OPEN** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/GP-ELFU Specification of Management Functions

FMT_SMF.1.1/GP-ELFU The TSF shall be capable of performing the following management functions

- **The Saving, Loading, Restore phases of the Executable Load File Process,**
- **Management of the ELF upgrade session status,**
- **Card management during the ELF upgrade session,**
- **[assignment: list of management functions to be provided by the TSF].**

FPT_FLS.1/GP-ELFU Failure with preservation of secure state

FPT_FLS.1.1/GP-ELFU The TSF shall preserve a secure state when the following types of failures occur:

- **The required minimum amount of memory is not available at the time the command MANAGE ELF UPGRADE is received,**
- **A fatal error occurs using the new ELF version during the Restore Phase,**
- **The ELF Upgrade Recovery Procedure fails,**
- **The installation of an Application instance fails,**
- **An interruption occurred during the Installation, Saving, Restore, or Consolidation Sequences,**
- **[assignment: list of types of failures in the TSF].**

16.5 Security Requirements Rationale

Table 16-4: Security Requirements Rationale of ELFU PP-Module

Security Objectives	SFRs	Rationale
O.ELF_AUTHORISED	FMT_MSA.1/GP-ELFU, FMT_MSA.3/GP-ELFU, FMT_SMF.1/GP-ELFU, FDP_ACC.1/GP-ELFU, FDP_ACF.1/GP-ELFU	Only the entity authenticated at the SD to which an ELF belongs can upgrade the ELF. That entity must have access rights to the security domain according to the ELF upgrade access control policy (FDP_ACC.1/GP-ELFU, FDP_ACF.1/GP-ELFU). FMT_MSA.3/GP-ELFU enforces the access control policy by providing restrictive default values for security attributes defined in FDP_ACF.1.1/GP-ELFU. FMT_MSA.1/GP-ELFU enforces the access control policy by restricting the ability to set and maintain the security attributes defined in FDP_ACF.1.1/GP-ELFU to the S.OPEN. FMT_SMF.1/GP-ELFU contributes to this objective by specifying the management functions available to load an authorised ELF
O.ELF_INTEGRITY	FIA_UID.1/GP, FDP_ACC.1/GP-ELFU, FDP_ACF.1/GP-ELFU	This security objective relates to the integrity of the upgraded ELF being loaded onto the platform, which is protected by the Secure Channel protocol (FIA_UID.1/GP) and the ELF upgrade access control policy (FDP_ACC.1/GP-ELFU, FDP_ACF.1/GP-ELFU).
O.ELF_APP_DATA	FPT_FLS.1/GP-ELFU	FPT_FLS.1/GP-ELFU contributes to this Objective as it prevents the use of corrupted application data.
O.ELF_SESSION	FMT_SMF.1/GP-ELFU, FIA_UID.1/GP	FMT_SMF.1/GP-ELFU contributes to this Objective by defining the start & end of the ELF_UPGRADE session. FIA_UID.1/GP specifies the actions that can be performed before the origin of the APDU commands that the card receives has been authorised.
O.ELF_DELE_IRR	FDP_ROL.1/GP-ELFU	FDP_ROL.1/GP-ELFU contributes to this Objective as it preserves the completion of the deletion operation.
O.ELF_DATA_PRO	FDP_RIP.1/ADEL	FDP_RIP.1/ADEL is used to ensure that contents of resources are only available to subjects having explicitly granted access to these resources.

16.6 SFR Dependencies

Table 16-5: SFR Dependencies of ELFU PP-Module

SFRs	CC Dependencies	Satisfied Dependencies
FMT_SMF.1/GP-ELFU	No Dependencies	No Dependencies
FPT_FLS.1/GP-ELFU	No Dependencies	No Dependencies
FMT_MSA.1/GP-ELFU	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/GP-ELFU FMT_SMR.1/GP FMT_SMF.1/GP-ELFU
FMT_MSA.3/GP-ELFU	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/GP-ELFU FMT_SMR.1/GP
FDP_ACC.1/GP-ELFU	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/GP-ELFU
FDP_ACF.1/GP-ELFU	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/GP-ELFU FMT_MSA.3/GP-ELFU
FDP_ROL.1/GP-ELFU	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control)	FDP_ACC.1/GP-ELFU

16.7 Consistency Rationale

The ELFU PP-Module is consistent with its the core SE PP and packages:

- The TOE type defined in the PP-Module is based on the TOE type defined in the core PP and packages.
- There are additional threats in the PP-Module, and there is no new assumption, which means that the PP-Module does not weaken the core PP and packages.
- There are additional objectives for the TOE, which do not contradict or invalidate the objectives of the core PP and packages.
- There are additional SFRs, which do not contradict or invalidate the SFRs of the core PP and packages.

17 PP-Module Amendment I: Secure Element Management Services (SEMS)

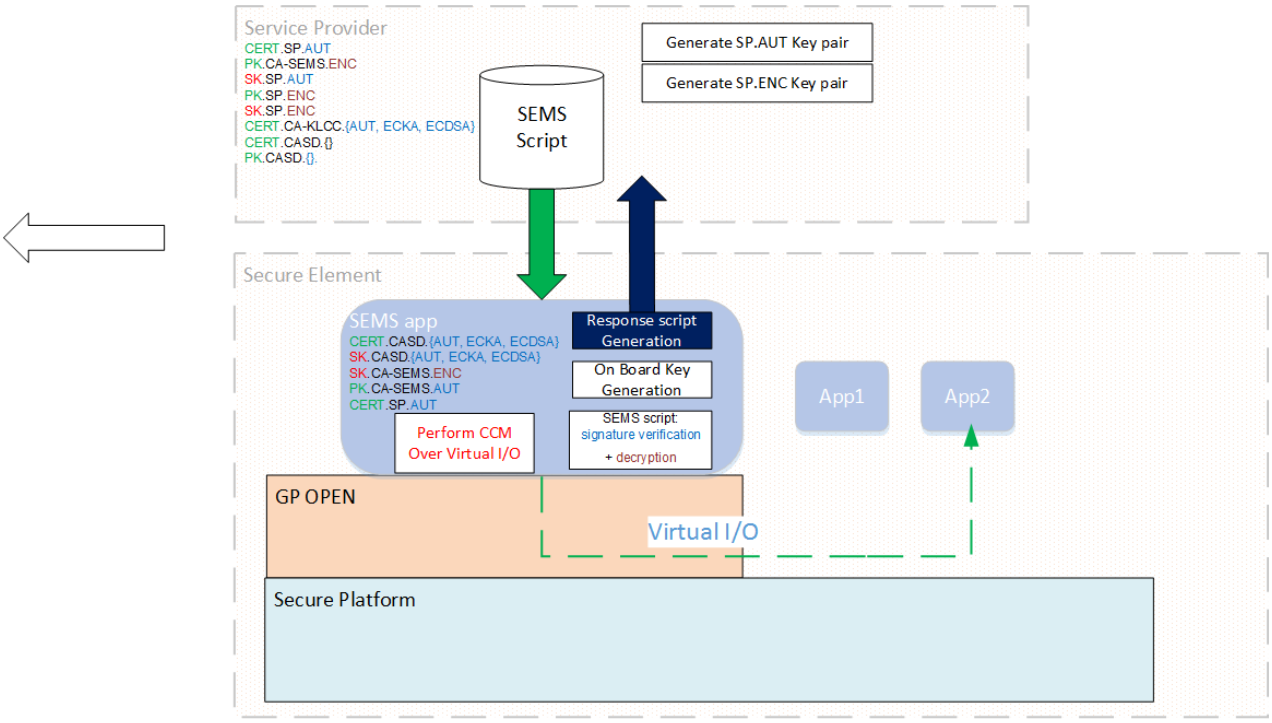
17.1 Scope

GlobalPlatform Amendment I [Amd I] defines the Secure Element Management Service, which provides a means to reduce the Card Content Management effort. The administration mechanism is migrated from an SEI TSM-based model to a Service Provider TSM-Centric model. The model changes from being a one-to-one continual synchronous relationship between the Service Provider and SE to a one-to-many, asynchronous relationship from Service Provider to many SEs.

[Amd I] augments the existing GlobalPlatform Delegation Model through the use of certificates.

The main simplification for Service Providers comes from the fact that SE diversified specific key data is no longer required to launch an administration session.

Figure 17-1: Amendment I: SEMS Components



17.1.1 SEMS Description

The SEMS Application is an on-card Application that can process SEMS commands. It may be implemented as either a Java Card applet or a Security Domain. The SEMS Application, regardless of its implementation as an SD or a Java Card applet, has the unique ability to forward APDUs via a virtual I/O interface. The OPEN shall grant access to the virtual I/O interface only to the SEMS Application and SEMS Updater.

17.1.2 SEMS Usage

For any given group of SEs which are managed via SEMS the Service Provider generates key pairs and certificates allowing only pre-defined GlobalPlatform Card Content Management (CCM) operations to be performed. The number of operations is limited and the operations can only be performed by those particular SEs through the SEMS having a key pair and certificate.

The following GlobalPlatform CCM operations may be delegated:

- Creation of Security Domains (with or without the Authorised Management privilege)
- Secure Channel key injection (on-board or off-board Key Generation) in SDs
- Loading and deletion of ELFs
- Instantiation and deletion of applets
- Applet personalisation with non-diversified data
- Key rotation of the SEMS on-card entity in case of change of ownership or for security reasons.

On receipt of a SEMS CCM script, each built-in certificate is checked by the SEMS Application residing on each SE.

17.1.3 SEMS Security Features

The SEMS Application implements integrity verification, authentication checking, and the decryption mechanism of the SEMS script; it enforces the CCM rights defined within the Service Provider certificate; and it processes the SEMS commands.

The SEMS commands and the responses to the execution of the SEMS commands are transferred to the SEMS Application by, respectively, the message and the response message of the PROCESS SCRIPT COMMAND APDU.

The SEMS Application is responsible for:

- Checking the authenticity and integrity of the SEMS script by verifying the CERT.SP.AUT and the signature of the SEMS script
- Integrity verification and decryption of the SEMS commands embedded in the SEMS script
- Enforcing the SEMS CCM rights defined in the CERT.SP.AUT contained in the SEMS script
- Processing the SEMS commands and forwarding the generated APDU to the Application selected with the SEMS_SELECT command through the Virtual I/O
- Retrieving the APDU response returned by the selected Application through the Virtual I/O and building the SEMS command response returned to the SEMS Agent in the PROCESS SCRIPT COMMAND APDU response.

17.2 SPD

SEMS is effectively an extension to Card Content Management and is able to support scenarios in support of Amendment A – Confidential Card Content Management [Amd A].

Table 17-1: SPDs of SEMS PP-Module

Assets	
D.SEMS-APPLICATION-CODE	The code of the SEMS application loaded on the card. To be protected from unauthorised modification.
D.SEMS-APPLICATION-DATA	The data (including personalisation) of the SEMS application loaded on the card. To be protected from unauthorised modification and disclosure.
D.SEMS-PUBLIC-KEYS	This stands for the following keys and certificates, which shall be protected from unauthorised modification: **CERT.CASD.{AUT, ECKA, ECDSA}** Certificate holding a public key PK.CASD.{AUT, ECKA, ECDSA} (per confidential key setting scheme supported), defined in section 4.5, used to verify the signature of the data returned by the SEMS Application. It is diversified per SE and stored within the SEMS Application and/or CASD. It can be retrieved by the SEMS_GET_DATA command. **PK.CA-SEMS.AUT** CA-SEMS public key (related to SK.CA-SEMS.AUT) used to verify the certificates signed by the CA-SEMS; i.e. CERT.SP.AUT. PK.CA-SEMS.AUT is stored in the SEMS Application. All SEs of a given group may share the same PK.CA-SEMS.AUT. **CERT.SP.AUT** Certificate, defined in section 4.5.1, provided to an SP by the CA-SEMS. It embeds the PK.SP.AUT used to verify the signature of the SEMS script. It contains the CCM rights assigned to the SP. **PK.SP.ENC.{S1,S4}** Service Provider public key (related to SK.SP.ENC.{S1,S4}) used to encrypt on-board generated keys returned by the SEMS Application. It is embedded in commands, defined in section 7.11 and 7.12, sent to the SEMS Application to trigger the on-board key generation. **PK.SP.ECKA.S3** Service Provider public key (related to SK.SP.ECKA.S3) used in the generation of a shared secret based on an ECKA algorithm. It is embedded in the command (defined in section 7.12) that is sent to the SEMS Application to trigger the on-board key generation.

D.SEMS-PRIVATE-KEYS	This stands for the following keys, which shall be protected from unauthorised modification and disclosure: **SK.CASD.{AUT, ECKA, ECDSA}** Private key set (related to PK.CASD.{AUT, ECKA, ECDSA} and securely stored in the SE) used by the SEMS Application to guarantee the authenticity and integrity of the on-board generated key returned by the SEMS Application. It is diversified per SE. **SK.CA-SEMS.ENC** CA-SEMS private key (related to PK.CA-SEMS.ENC and stored in the SE) used by the SEMS Application to decrypt an incoming SEMS script. The same SK.CA-SEMS.ENC is used for a given group of SEs.
Subjects	
S.CA-SEMS	**SEMS Certification Authority** Manage the CA-SEMS.AUT and CA-SEMS.ENC key pairs. Release CERT.SP.AUT certificate(s) to a Service Provider on receipt of a Certificate Signing Request issued by a Service Provider.
S.CA-KLCC	**Key Loading Card Certificates Certificate Authority** Manage the CA-SEMS.AUT and CA-SEMS.ENC key pairs. Release CA-KLCC certificate(s), to a Service Provider on its request, so that the Service Provider can verify the (data origin) authenticity of the SEMS Application responses.
S.SP-SEMS	**Service Provider** The Service Provider deploys and operates services on groups of SEs. The Card Content Management scope is defined through CERT.SP.AUT certificates that are generated and provided by the CA-SEMS. The Service Provider (also referred to as the SEMS SP certificate holder) generates, secures, and broadcasts generic SEMS scripts to MEs, thus allowing the execution of standard GlobalPlatform CCM operations on groups of SEs. A SEMS script is a collection of CERT.SP.AUT certificate(s), frame(s) containing the script signature and data used to decrypt the SEMS commands, and encrypted and integrity-protected SEMS commands.
S.AP-SEMS	**SEMS Application Provider** The SEMS Application Provider, functioning as a special Service Provider (SP), is responsible for installing and provisioning the SEMS Application. It has a strong trust relationship to the CA-SEMS and may be authorised to rotate the CA-SEMS keys or, if the SEMS Application is implemented as a Java Card applet, to update the SEMS Application using the SEMS Updater.

Threats	
T.SEMS-IMPERSONATE	Threat agent: Attacker Adverse action: An Attacker tries to impersonate a SEMS script or corrupt the content of a SEMS script. Directly threatened asset(s): All SEMS PP-Module assets are threatened. *Application Note*: [Amd I] augments existing card management activities within secured scripts, the threat against this is impersonation of a SEMS script or corruption of a SEMS script.
Assumptions	
A.SEMS-SERVICE-PROVIDER	The SEMS Service Provider maintains a secure environment where SK.CA-SEMS.AUT is stored and used to sign CERT.SP.AUT certificates.
A.SEMS-APPS-PROVIDER	The SEMS Application Provider maintains a secure environment where SK.SP.AUT is stored and used to sign SEMS scripts.

Application Note:

SEMS relies upon the correct implementation of a virtual I/O interface, allowing an on-card entity (SD / Application instance) to process SEMS commands for the application exactly as if they were sent directly via a physical I/O Interface, and enables the SEMS Application to forward GlobalPlatform CCM commands to specific Security Domains.

17.3 Objectives

The security of the [Amd I] functionality is based on a strong trust relationship between the SEMS Application provider and the SEMS Certification Authority (CA-SEMS).

Table 17-2: Objectives of SEMS PP-Module

Security Objectives for the TOE	
O.SEMS-CCCM	The TOE shall support the confidential key setting scheme defined in section 4.8.2.1 of [Amd I]. The TOE may support the GlobalPlatform confidential key setting scenarios #1 and #3 defined in [Amd A].
O.SEMS-SCRIPT-AUTH	The TOE shall verify the SEMS script Authenticity and origin by verifying the CERT.SP.AUT and signature.
O.SEMS-COMMAND-AUTH	The TOE shall decrypt and verify integrity of SEMS commands embedded in the SEMS script.
O.SEMS-OPEN	The OPEN shall provide a virtual I/O interface for exclusive use of only the SEMS Application and SEMS Updater to perform management functions on target apps, for which the OPEN will perform trust relationship matching on behalf of, before routing the APDUs to the target application. The OPEN shall verify that the CERT.SP.AUTH embedded in the SEMS script matches that which is loaded on the target application, before routing the C-APDUs to the application.

Security Objectives for the Operational Environment	
OE.SEMS-SERVICE-PROVIDER	The SEMS Service Provider shall maintain a secure environment where SK.CA-SEMS.AUT is stored and used to sign CERT.SP.AUT certificates.
OE.SEMS-APPS-PROVIDER	The SEMS Application Provider shall maintain a secure environment where SK.SP.AUT is stored and used to sign SEMS scripts.

17.3.1 Security Objectives Rationale

Table 17-3: Security Objectives Rationale of SEMS PP-Module

Threats, Assumptions	Objectives	Rationale
T.SEMS-IMPERSONATE	O.SEMS-CCCM, O.SEMS-SCRIPT-AUTH, O.SEMS-COMMAND-AUTH, O.SEMS-OPEN	O.SEMS-CCCM provides various confidential key setting schemes to setup and personalise secure channel keys in a secure domain and protect the SEMS script. O.SEMS-SCRIPT-AUTH provides a means to verify the SEMS script Authenticity and origin. O.SEMS-COMMAND-AUTH provides a means to decrypt and verify integrity of SEMS commands embedded in the SEMS script. O.SEMS-OPEN ensures that only SEMS Application and SEMS Updater are authorised to use a virtual I/O interface provided by the OPEN to perform management functions on target apps.
A.SEMS-SERVICE-PROVIDER	OE.SEMS-SERVICE-PROVIDER	OE.SEMS-SERVICE-PROVIDER requires a secure environment to be provided by the SEMS Service Provider for the protection of SK.CA-SEMS.AUT used to sign CERT.SP.AUT certificates.
A.SEMS-APPS-PROVIDER	OE.SEMS-APPS-PROVIDER	OE.SEMS-APPS-PROVIDER requires a secure environment to be provided by the SEMS Application Provider for the protection of SK.SP.AUT used to sign SEMS scripts.

17.4 Security Functional Requirements

SEMS provides a means to securely send scripts for CCM and CCCM reusing the functionality already in place for those features. A Secure implementation of SEMS relies upon the Asymmetric cryptography described in [Amd I] and the implementation of the Virtual I/O channel providing a route for the SEMS scripts from the SEMS application to the target application.

FCS_CKM.1/SEMS-ECC Cryptographic key generation

FCS_CKM.1.1/SEMS-ECC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**

Application Note:

This SFR stands for the generation of a semi-static ECC key pair (r, R) by the SEMS Application. The (static) private key r of the semi-static ECC key pair and the public key PK.SP.ENC.S4 are used to compute a Shared Secret using the ECDH cryptographic algorithm.

FCS_CKM.1/SEMS-SCP Cryptographic key generation

FCS_CKM.1.1/SEMS-SCP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**

Application Note:

This SFR stands for the generation of SCP02 or SCP03 Security Domain keys (K_{ENC}, K_{MAC}, K_{DEC}). These keys are derived from RGK.

FCS_RNG.1/SEMS-RGK Random numbers generation

FCS_RNG.1.1/SEMS-RGK The TSF shall provide a **[selection: physical, non-physical true, deterministic, hybrid, hybrid deterministic]** random number generator **[selection: DRG.2, DRG.3, DRG.4, PTG.2, PTG.3, NTG.1] [AIS20] [AIS31]** that implements: **[assignment: list of security capabilities]**.

FCS_RNG.1.2/SEMS-RGK The TSF shall provide random numbers that meet **[assignment: a defined quality metric]**.

Application Note:

This SFR stands for the generation of the on-board RGK (Randomly Generated Key). The SEMS_PULL_KEY command triggers the on-board key generation process. The SEMS Application performs this random key generation on the SE to derive SCP keys as described in section 4.8.2.1.1 of [Amd I].

This SFR corresponds to FCS_RNG.1 of [PP-JC], applied to SEMS (this is why it has been renamed).

FCS_COP.1/SEMS Cryptographic operation

FCS_COP.1.1/SEMS The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**

Application Note:

- The ST writer may define one FCS_COP.1/SEMS for all the cryptographic operations involved in the implementation of SEMS or one per operation.
- For instantiating the SFR, the ST writer should use the table below to select the cryptographic operations, algorithms, key sizes, and recommended standards implemented by the SE.
- The ST writer should check the cryptographic operations implemented by the TOE against the GlobalPlatform Cryptographic Algorithm Recommendations [GP Crypto].

Table 17-4: Cryptographic Operations Involved in Implementation of SEMS

Operation	Algorithm	Length	Recommended Standards
Key Decryption (Decrypt the AES key K_n concatenated with the SEMS command using the AES cryptographic algorithm in the CBC mode with the former stored AES key K_{n-1})	AES in CBC mode	128 bits	[NIST 800-38A]
Message Authentication Code	CMAC AES	128, 192, or 256 bits	[NIST 800-38B] and [FIPS 140-2]
Hashing (Verify the integrity of the SEMS command by comparing the latest retrieved SHA-256 with the computed SHA-256)	SHA	SHA-256	[NIST 800-57]
Digital Signature Verification (PK.SP.AUT included in the CERT.SP.AUT certificate and embedded in the SEMS scripts is used to verify the SEMS script signature by SEMS Application)	ECDSA	256, 384, 512, or 521 bits	[GPCS] section B.4.3.
Confidential key setting (mandatory): SEMS Confidential Set-up of Secure Channel Key Set ([Amd I] section 4.8.2.1)			
Key Derivation (Derive the AES key K from the computed shared secret using the KDF function described in [Amd I] section 4.6.3.5)	CMAC-based KDF using AES	128 bits	[NIST 800-56B]
Computation of a Shared Secret (ShS) using the ECDH of the (static) private key r of the semi-static ECC key pair and the public key PK.SP.ENC.S4	ECKA-DH	256, 384, 512, or 521 bits	[TR 03111]
Signature generation using the ECDSA private key SK.CASD.ECDSA. The signature is computed over the concatenation of the semi-static ECC key R, the AES Encrypted RGK with the AES key K, the SD AID, and the SE SN (sign (R|| AES[K,RGK] || SD AID || SE SN))	ECDSA	256, 384, 512, or 521 bits	[GPCS] section B.4.3

Operation	Algorithm	Length	Recommended Standards
Encryption of the RGK using the key K	AES	128 bits	[NIST 800-38A]
Confidential key setting (optional): Variant based on GlobalPlatform Amendment A Scenario #1 ([Amd l] section 4.8.2.2)			
Derivation of SCP keys from the RGK, defined in [Amd A] section 3.5.2.	AES	128 bits	[NIST 800-38A]
Encryption of the RGK using the PK.SP.ENC.S1 key [Amd A] section 3.5.2.	RSAES-PKCS1-v1_5 or RSAES-OAEP	1024 to 4096 bits	[GPCS] or [GPCS] section B.3.2.2.
Signature of the RGK with the SK.CASD.AUT private key	RSASSA-PSS	1024 to 4096 bits	[Amd A] section 3.5.2. [GPCS] section B.3.2.1.
Confidential key setting (optional): SEMS Implementation of GlobalPlatform Amendment A Scenario #3 ([Amd l] section 4.8.2.3)			
Computation of the ShS from PK.AP.ECKA.S3 and SK.CASD.ECKA (EC Key Agreement)	ECKA-DH protocol	256, 384, 512, or 521 bits	[TR 03111]
Derivation of SCP keys from ShS	SHA-256	N/A	[NIST 800-56A]
Computation of the receipt	AES-128	128 bits	[NIST 800-38B]

See recommendations 1 to 3 from Table 2-1.

FCO_NRO.2/SEMS Enforced proof of origin

FCO_NRO.2.1/SEMS The TSF shall enforce the generation of evidence of origin for transmitted **SEMS Scripts** at all times.

FCO_NRO.2.2/SEMS The TSF shall be able to relate the **CERT.SP.AUT in the SEMS script** of the originator of the information, and the **CERT.SP.AUT in the registry** of the information to which the evidence applies.

FCO_NRO.2.3/SEMS The TSF shall provide a capability to verify the evidence of origin of information to **the originator** given **at the time the SEMS script is processed.**

FMT_SMR.1/SEMS Security roles

FMT_SMR.1.1/SEMS The TSF shall maintain the roles:

- **Off-card: S.CA-SEMS, S.CA-KLCC, S.SP_SEMS, S.AP_SEMS**
- **On-card: S.OPEN, SEMS Application, Target Application.**

FMT_SMR.1.2/SEMS The TSF shall be able to associate users with roles.

FMT_SMF.1/SEMS Specification of management functions

FMT_SMF.1.1/SEMS The TSF shall be capable of performing the following management functions:

- **Transmit SEMS Card Content Management APDUs and SEMS commands over a Virtual I/O channel.**

Application Note:

Command and Response APDUs exchanged between the SEMS Device Agent and the SEMS Application are defined in [Amd I] sections 6 and 7.

FDP_ACC.1/SEMS Subset access control

FDP_ACC.1.1/SEMS The TSF shall enforce the **SEMS CCM Access Control Policy** on **the following list of subjects, objects, and operations:**

- **Subjects: SEMS Application (Java Card applet or a Security Domain), S.OPEN, Target Application, SEMS Updater**
- **Objects: SEMS scripts**
- **Operation controlled by the policy: SEMS Application APDUs and SEMS commands.**

Application Note:

APDU commands are described in [Amd I] sections 6 and 7.

FDP_ACF.1/SEMS Security attribute based access control

FDP_ACF.1.1/SEMS The TSF shall enforce the **SEMS CCM Access Control Policy** to objects based on the following:

- **Security Attributes: SEMS Application states (SELECTABLE, PERSONALIZED), Target Application states, Authentication states, Security levels of the secured SEMS script ((AUTHENTICATED || C_MAC || C_DECRYPTION and conditionally R_MAC || R_ENCRYPTION).**

FDP_ACF.1.2/SEMS The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The OPEN grants access to the virtual I/O interface only to the SEMS Application and SEMS Updater.**
- **The SEMS Application only considers the CCM rights and licenses within the CERT.SP.AUT that is used to authenticate the currently executed SEMS script.**

- **The SEMS Application terminates an authentication session and resets the authentication state (e.g. clear session keys and chaining data), on any of the following:**
    - **A failed verification of a CERT.SP.AUT certificate.**
    - **A failed verification of the integrity of a secured SEMS command.**
- **All personalisation commands are executed to consider that the personalisation performed via SEMS script processing is complete. If the personalisation sequence is interrupted because of a power loss or reset of the SE or a failed SEMS command, the SEMS Application deletes the Application instance referenced in SEMS_BEGIN_PERSO on receipt of the first verification of the Authentication Frame.**
- **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

FDP_ACF.1.3/SEMS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/SEMS The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].**

FMT_MSA.1/SEMS Management of security attributes

FMT_MSA.1.1/SEMS The TSF shall enforce the **SEMS CCM Access Control Policy** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **defined in FDP_ACF.1.1/SEMS** to the **[assignment: the authorised identified roles].**

FMT_MSA.3/SEMS Security attribute initialization

FMT_MSA.3.1/SEMS The TSF shall enforce the **SEMS CCM Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SEMS The TSF shall allow the **[assignment: the authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

17.5 Security Requirements Rationale

Table 17-5: Security Requirements Rationale of SEMS PP-Module

Security Objectives	SFRs	Rationale
O.SEMS-CCCM	FCS_CKM.1/SEMS-ECC, FCS_CKM.1/SEMS-SCP, FCS_RNG.1/SEMS-RGK, FCS_COP.1/SEMS	FCS_CKM.1/SEMS-ECC addresses the generation of a semi-static ECC key pair (r, R) by the SEMS Application. FCS_CKM.1/SEMS-SCP addresses the generation of SCP02 or SCP03 Security Domain keys (K_{ENC}, K_{MAC}, K_{DEC}). FCS_RNG.1/SEMS-RGK addresses the generation of the on-board RGK (Randomly Generated Key). FCS_COP.1/SEMS specifies the cryptographic algorithms used by SEMS services.
O.SEMS-SCRIPT-AUTH	FCS_COP.1/SEMS, FCO_NRO.2/SEMS	FCS_COP.1/SEMS specifies the cryptographic algorithms used by SEMS services. FCO_NRO.2/SEMS generates an evidence of origin for transmitted SEMS Scripts at all times.
O.SEMS-COMMAND-AUTH	FCS_COP.1/SEMS, FDP_ACC.1/SEMS, FDP_ACF.1/SEMS, FMT_MSA.1/SEMS, FMT_MSA.3/SEMS, FMT_SMF.1/SEMS, FMT_SMR.1/SEMS	FCS_COP.1/SEMS specifies the cryptographic algorithms used by SEMS services. FDP_ACC.1/SEMS and FDP_ACF.1/SEMS enforce the SEMS CCM Access Control Policy for managing SEMS script. FMT_MSA.1/SEMS enforces the SEMS CCM Access Control Policy by restricting the ability to set and maintain the security attributes defined in FDP_ACF.1.1/SEMS to the S.OPEN. FMT_MSA.3/SEMS enforces the SEMS CCM Access Control Policy by providing restrictive default values for security attributes defined in FDP_ACF.1.1/SEMS. FMT_SMF.1/SEMS enforces the management of the transmitted SEMS Card Content Management APDUs and SEMS commands over a Virtual I/O channel. FMT_SMR.1/SEMS maintains the roles: • Off-card: S.CA-SEMS, S.CA-KLCC, S.SP_SEMS, S.AP_SEMS • On-card: S.OPEN, SEMS Application, Target Application

Security Objectives	SFRs	Rationale
O.SEMS-OPEN	FDP_ACC.1/SEMS, FDP_ACF.1/SEMS, FMT_MSA.1/SEMS, FMT_MSA.3/SEMS, FMT_SMF.1/SEMS, FMT_SMR.1/SEMS	FDP_ACC.1/SEMS and FDP_ACF.1/SEMS enforce the SEMS CCM Access Control Policy for managing SEMS script. FMT_MSA.1/SEMS enforces the SEMS CCM Access Control Policy by restricting the ability to set and maintain the security attributes defined in FDP_ACF.1.1/SEMS to the S.OPEN. FMT_MSA.3/SEMS enforces the SEMS CCM Access Control Policy by providing restrictive default values for security attributes defined in FDP_ACF.1.1/SEMS. FMT_SMF.1/SEMS enforces the management of the transmitted SEMS Card Content Management APDUs and SEMS commands over a Virtual I/O channel. FMT_SMR.1/SEMS maintains the roles: • Off-card: S.CA-SEMS, S.CA-KLCC, S.SP_SEMS, S.AP_SEMS • On-card: S.OPEN, SEMS Application, Target Application

17.6 SFR Dependencies

Table 17-6: SFR Dependencies of SEMS PP-Module

SFRs	CC Dependencies	Satisfied Dependencies
FCS_CKM.1/SEMS-ECC	(FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SEMS FCS_CKM.4 (from [PP-JC])
FCS_CKM.1/SEMS-SCP	(FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/SEMS FCS_CKM.4 (from [PP-JC])
FCS_RNG.1/SEMS-RGK	No dependencies	No Dependencies
FCS_COP.1/SEMS	(FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/SEMS-ECC FCS_CKM.1/SEMS-SCP FCS_CKM.4 (from [PP-JC])
FCO_NRO.2/SEMS	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FDP_ACC.1/SEMS	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/SEMS
FDP_ACF.1/SEMS	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/SEMS FMT_MSA.3/SEMS
FMT_MSA.1/SEMS	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1/SEMS FMT_SMR.1/SEMS FMT_SMF.1/SEMS
FMT_MSA.3/SEMS	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/SEMS FMT_SMR.1/SEMS
FMT_SMF.1/SEMS	No dependencies	No dependencies
FMT_SMR.1/SEMS	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FIA_UID.1	No dependencies	No dependencies

17.7 Consistency Rationale

The SEMS PP-Module is consistent with the core SE PP and packages:

- The TOE type defined in the PP-Module is based on the TOE type defined in the core PP and packages.

- There are additional threats and OSPs in the PP-Module which do not contradict the core PP and packages.
- There are two new assumptions in the PP-Module related to the extended scope, therefore this does not weaken the core PP and packages.
- There are additional objectives for the TOE, which do not contradict or invalidate the objectives of the core PP and packages.
- There are additional objectives for the environment, which do not weaken the core PP and packages since these are related to the extended scope.
- There are additional SFRs, which do not contradict or invalidate the SFRs of the core PP and packages.

18 PP-Module OS Update

18.1 Scope

This PP-Module addresses the security requirements related to the OS update capability, especially when such a capability is available post-issuance.

This PP-Module does not address the situation where an entire OS would be replaced as supported in the Package 'Loader' from the [PP-0084]. Only an OS update is covered by this module, not an OS replacement.

The TOE type is an SE with OS Update capability.

Terminology:

- The term "OS" designates the TOE full operating system, composed of the native layer, the Java Card system, and the GlobalPlatform Framework. Some additional plugins might be present in the OS to address specific needs at the operating system level.
- The term "OS Update" refers to the TOE capability of loading, installing, and activating additional code on the OS. Such additional code might be necessary to fix an issue or to add new functionalities.
- The term "Initial TOE" refers to the evaluated and certified TOE, whose OS Update capability has been assessed according to the present security requirements.
- After additional code has been loaded, installed, and activated, the "Initial TOE" becomes the "Updated TOE".

Actors:

- **OS Developer:** The actor that developed the OS of the Initial TOE. Should an OS Update be needed, it is assumed that the related additional code would be developed by the same actor.
- **Issuer:** The actual owner of the SE. As such, no OS Update operation shall be made without the Issuer's consent. This concept has been introduced in the core PP.
- For the separation of roles, the OS Developer shall own dedicated cryptographic keys to ensure the confidentiality of the additional code transmitted to the TOE and to verify its authenticity and integrity.

Any TOE providing the OS Update capability shall enforce the security requirements outlined in this PP-Module. From a technical perspective, how these requirements are enforced (i.e. how the corresponding security functions are implemented) is out of scope of this document. Although the GlobalPlatform specifications offer a variety of mechanisms that can be used to enforce the requirements, the OS Developer is not mandated to rely on them and is free to implement any proprietary solution, provided that the security requirements contained in this PP-Module are met.

18.2 SPD

Table 18-1: SPDs of the OS Update PP-Module

Assets	
D.OS-UPDATE_SGNVER-KEY	Refinement of D.APP_KEYS. A cryptographic key, owned by the OS Developer, and used by the TOE to verify the signature of the additional code to be loaded.

	Note: No assumption is made on the type of this signature verification key, i.e. it can be either a symmetric key or the public component of an asymmetric key pair. In case of a symmetric key: to be protected from unauthorised disclosure and modification. In case of an asymmetric public key: to be protected from unauthorised modification.
D.OS-UPDATE_DEC-KEY	Refinement of D.APP_KEYS. A cryptographic key, owned by the OS Developer, and used by the TOE to decrypt the additional code to be loaded. Note: No assumption is made on the type of this decryption key, i.e. it can be either a symmetric key or the secret component of an asymmetric key pair. To be protected from unauthorised disclosure and modification.
D.OS-UPDATE_ADDITIONALCODE	The code to be added to the OS after TOE issuance. The additional code has to be signed by the OS Developer. After successful verification of the signature by the Initial TOE, the additional code is loaded and installed through an atomic activation (to create an Updated TOE). To be protected from unauthorised disclosure and modification.
D.OS-UPDATE-CODE-ID	The identification data associated with the additional code. It is loaded and/or updated in the same atomic operation as additional code loading. To be protected from unauthorised modification. *Application Note*: The identification data (D.OS-UPDATE-CODE-ID) may also be protected from unauthorised disclosure (confidentiality requirement) by not permitting an attacker to determine whether a given TOE has been updated or not (even if it is not possible to distinguish between functional and security updates). However, confidentiality is not mandatory since in most cases the identification data must be readily available on the field through technical commands, even in the TERMINATED state.
Threats	
T.UNAUTHORISED-TOE-CODE-UPDATE	Threat agent: Attacker Adverse action: An attacker loads malicious additional code in order to compromise the security features of the TOE. Directly threatened asset(s): D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.
T.FAKE-SGNVER-KEY	Threat agent: Attacker

	Adverse action: An attacker modifies the signature verification key used by the TOE to verify the signature of the additional code. Hence, the attacker is able to sign and successfully load malicious additional code inside the TOE. Directly threatened asset(s): D.OS-UPDATE_SGNVER-KEY, D.OS-UPDATE_ADDITIONALCODE.
T.WRONG-UPDATE-STATE	Threat agent: Attacker Adverse action: An attacker prevents the OS Update operation to be performed atomically, resulting in an inconsistency between the resulting TOE code and the identification data: • The additional code is not loaded within the TOE, but the identification data is updated to mention that the additional code is present. • The additional code is loaded within the TOE, but the identification data is not updated to indicate the change. Directly threatened asset(s): D.OS-UPDATE-CODE-ID.
T.INTEG-OS-UPDATE-LOAD	Threat agent: Attacker Adverse action: The attacker modifies (part of) the additional code when it is transmitted to the TOE for installation. Directly threatened asset(s): D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.
T.CONFID-OS-UPDATE-LOAD	Threat agent: Attacker Adverse action: The attacker discloses (part of) the additional code when it is transmitted to the TOE for installation. Directly threatened asset(s): D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.
Organisational Security Policies	
OSP.ATOMIC_ACTIVATION	Additional code has to be loaded and installed on the Initial TOE through an atomic activation to create the Updated TOE. Each additional code shall be identified with unique Identification Data. During such atomic activation, identification Data of the Initial TOE have to be updated to clearly identify the Updated TOE. In case of interruption or incident during activation, the TOE shall remain in its initial state or fail secure.
OSP.TOE_IDENTIFICATION	Identification Data of the resulting Updated TOE shall identify the Initial TOE and the activated additional code. Identification Data shall be protected in integrity.
OSP.ADDITIONAL_CODE_SIGNING	The additional code has to be signed with a cryptographic key according to relevant standards, and the generated signature is associated with the additional code.

	The additional code signature must be verified during loading to assure its authenticity and integrity and to assure that loading is authorised on the TOE. The cryptographic key used to sign the additional code shall be of sufficient quality and its generation shall be appropriately secured to ensure the authenticity, integrity, and confidentiality of the key.
OSP.ADDITIONAL_CODE_ENCRYPTION	The additional code has to be encrypted according to the relevant standard in order to ensure its confidentiality when it is transmitted to the TOE for loading and installation. The encryption key shall be of sufficient quality and its generation shall be appropriately secured to ensure the confidentiality, authenticity, and integrity of the key.
Assumptions	
A.OS-UPDATE-EVIDENCE	For additional code loaded pre-issuance, it is assumed that evaluated technical and/or audited organisational measures have been implemented to ensure that the additional code: 1. has been issued by the genuine OS Developer 2. has not been altered since it was issued by the genuine OS Developer. For additional code loaded post-issuance, it is assumed that the OS Developer provides digital evidence to the TOE in order to prove the following: 1. he is the genuine developer of the additional code and 2. the additional code has not been modified since it was issued by the genuine OS Developer.
A.SECURE_ACODE_MANAGEMENT	It is assumed that: • The Key management process related to the OS Update capability takes place in a secure and audited environment. • The cryptographic keys used by the cryptographic operations are of strong quality and appropriately secured to ensure confidentiality, authenticity, and integrity of those keys.

18.3 Objectives

Table 18-2: Objectives of OS Update PP-Module

Security Objectives for the TOE	
O.SECURE_LOAD_ACODE	The TOE shall check an evidence of authenticity and integrity of the additional code to be loaded. The TOE enforces that only an allowed version of the additional code can be loaded. The TOE shall forbid the loading of an additional code not intended to be assembled with the TOE.

	During the loading of the additional code, the TOE shall remain secure.
O.SECURE_AC_ACTIVATION	Activation of the additional code and update of the Identification Data shall be performed at the same time in an atomic way. All the operations needed for the code to be able to operate as in the Updated TOE shall be completed before activation. If the atomic activation is successful, then the resulting product is the Updated TOE, otherwise (in case of interruption or incident which prevents the forming of the Updated TOE), the TOE shall preserve a secure state.
O.TOE_IDENTIFICATION	The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After atomic activation of the additional code, the Identification Data of the Updated TOE allows identifications of both the Initial TOE and additional code. The user must be able to uniquely identify Initial TOE and additional code(s) which are embedded in the Updated TOE.
O.CONFID-OS-UPDATE.LOAD	The TOE shall decrypt the additional code prior installation. *Application Note*: Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION later in this table). Confidentiality protection can be achieved either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.
Security Objectives for the Operational Environment	
OE.OS-UPDATE-EVIDENCE	For additional code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organisational measures must ensure that the additional code (1) has been issued by the genuine OS Developer and (2) has not been altered since it was issued by the genuine OS Developer. For additional code loaded post-issuance, the OS Developer shall provide digital evidence to the TOE that (1) he is the genuine developer of the additional code and (2) the additional code has not been modified since it was issued by the genuine OS Developer.
OE.OS-UPDATE-ENCRYPTION	For additional code loaded post-issuance, the OS Developer shall encrypt the additional code so that its confidentiality is ensured when it is transmitted to the TOE for loading and installation.
OE.SECURE_ACODE_MANAGEMENT	Key management processes related to the OS Update capability shall take place in a secure and audited environment. The key generation processes shall guarantee that cryptographic keys are of sufficient quality and appropriately secured to ensure confidentiality, authenticity, and integrity of the keys.

18.3.1 Security Objectives Rationale

Table 18-3: Security Objectives Rationale of OS Update PP-Module

Threats, OSPs, Assumptions	Objectives	Rationale
T.UNAUTHORISED-TOE-CODE-UPDATE	O.SECURE_LOAD_ACODE	O.SECURE_LOAD_ACODE ensures that only an allowed version of the additional code can be loaded.
T.FAKE-SGNVER-KEY	O.SECURE_LOAD_ACODE	O.SECURE_LOAD_ACODE ensures that only an allowed version of the additional code can be loaded.
T.INTEG-OS-UPDATE-LOAD	O.SECURE_LOAD_ACODE	O.SECURE_LOAD_ACODE ensures that only an allowed version of the additional code can be loaded.
T.WRONG-UPDATE-STATE	O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION	O.SECURE_AC_ACTIVATION ensures that the activation of the additional code and update of the Identification Data are performed at the same time in an atomic way. O.TOE_IDENTIFICATION guarantees the integrity of the stored Identification Data in its non-volatile memory.
T.CONFID-OS-UPDATE-LOAD	O.CONFID-OS-UPDATE.LOAD	O.CONFID-OS-UPDATE.LOAD performs the decryption of the additional code prior installation.
OSP.ATOMIC_ACTIVATION	O.SECURE_AC_ACTIVATION	O.SECURE_AC_ACTIVATION ensures that the activation of the additional code and update of the Identification Data are performed at the same time in an atomic way.
OSP.ADDITIONAL_CODE_SIGNING	O.SECURE_LOAD_ACODE	O.SECURE_LOAD_ACODE ensures that only an allowed version of the additional code can be loaded.
OSP.TOE_IDENTIFICATION	O.TOE_IDENTIFICATION	O.TOE_IDENTIFICATION guarantees the integrity of the stored Identification Data in its non-volatile memory.

Threats, OSPs, Assumptions	Objectives	Rationale
OSP.ADDITIONAL_CODE_ ENCRYPTION	O.CONFID-OS-UPDATE.LOAD, OE.OS-UPDATE-ENCRYPTION	O.CONFID-OS-UPDATE.LOAD performs the decryption of the additional code prior installation. OE.OS-UPDATE-ENCRYPTION requires confidentiality protection measures on the additional code loaded when it is transmitted to the TOE for loading and installation.
A.OS-UPDATE-EVIDENCE	OE.OS-UPDATE-EVIDENCE	OE.OS-UPDATE-EVIDENCE requires integrity protection measures on the additional code loaded
A.SECURE_ACODE_ MANAGEMENT	OE.SECURE_ACODE_ MANAGEMENT	OE.SECURE_ACODE_ MANAGEMENT ensures that a key management process related to the OS Update capability is in place in a secure and audited environment.

18.4 Security Functional Requirements

FDP_ACC.1/OS-UPDATE Subset access control

FDP_ACC.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** on **the following list of subjects, objects, and operations**:

- **Subjects: S.OS-DEVELOPER is the representative of the OS Developer within the TOE, being responsible for signature verification and decryption of the additional code, before:**
  - **Loading**
  - **Installation**
  - **Activation**
  - **[assignment: list of other subjects covered by the SFP]**

  is authorised.
- **Objects: additional code and associated cryptographic signature**
- **Operations: loading, installation, and activation of additional code.**

FDP_ACF.1/OS-UPDATE Security attribute based access control

FDP_ACF.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to objects based on the following:

- **Security Attributes**:
    - **The additional code cryptographic signature verification status**
    - **The Identification Data verification status (between the Initial TOE and the additional code).**

FDP_ACF.1.2/OS-UPDATE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The verification of the additional code cryptographic signature (using D.OS-UPDATE_SGNVER-KEY) by S.OS-DEVELOPER is successful.**
- **The decryption of the additional code prior installation (using D.OS-UPDATE_DEC-KEY) by S.OS-DEVELOPER is successful.**
- **The comparison between the identification data of both the Initial TOE and the additional code demonstrates that the OS Update operation can be performed.**
- **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

FDP_ACF.1.3/OS-UPDATE The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/OS-UPDATE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].**

Application Note:

Identification data verification is necessary to ensure that the received additional code is actually targeting the TOE and that its version is compatible with the TOE version.

Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION). Confidentiality protection can be achieved either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

FMT_MSA.3/OS-UPDATE Security attribute initialization

FMT_MSA.3.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/OS-UPDATE The TSF shall allow the **OS Developer** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

The additional code signature verification status must be set to “Fail” by default. This prevents installation of any additional code until the additional code signature is successfully verified by the TOE.

FMT_SMR.1/OS-UPDATE Security roles

FMT_SMR.1.1/OS-UPDATE The TSF shall maintain the roles **OS Developer, Issuer**.

FMT_SMR.1.2/OS-UPDATE The TSF shall be able to associate users with roles.

FMT_SMF.1/OS-UPDATE Specification of Management Functions

FMT_SMF.1.1/OS-UPDATE The TSF shall be capable of performing the following management functions: **activation of additional code**.

Application Note:

Once verified and installed, additional code needs to be activated to become effective.

FIA_ATD.1/OS-UPDATE User attribute definition

FIA_ATD.1.1/OS-UPDATE The TSF shall maintain the following list of security attributes belonging to individual users: **additional code ID for each activated additional code**.

Refinement: "Individual users" stands for additional code.

FTP_TRP.1/OS-UPDATE Trusted Path

FTP_TRP.1.1/OS-UPDATE The TSF shall provide a communication path between itself and **remote** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[selection: disclosure, none]**.

FTP_TRP.1.2/OS-UPDATE The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/OS-UPDATE The TSF shall require the use of the trusted path for **the transfer of the additional code to the TOE**.

Application Note:

During the transmission of the additional code to the TOE for loading, the confidentiality shall be ensured either through direct encryption of the additional code, or by means of a trusted path ensuring the confidentiality of the communication to the TOE.

If the additional code is encrypted independently of the trusted path, the ST writer can select ‘none’ in FTP_TRP.1.1/OS-UPDATE.

Otherwise, the trusted path shall ensure the confidentiality of the transmitted additional code. In this case the ST writer shall select ‘disclosure’ in FTP_TRP.1.1/OS-UPDATE.

FCS_COP.1/OS-UPDATE-DEC Cryptographic operation

FCS_COP.1.1/OS-UPDATE-DEC The TSF shall perform **Decryption of the additional code prior installation** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

FCS_COP.1/OS-UPDATE-VER Cryptographic operation

FCS_COP.1.1/OS-UPDATE-VER The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

FPT_FLS.1/OS-UPDATE Failure with preservation of secure state

FPT_FLS.1.1/OS-UPDATE The TSF shall preserve a secure state when the following types of failures occur: **interruption or incident which prevents the forming of the Updated TOE**.

Application Note:

The OS Update operation must either be successful or fail securely. The TOE code and identification data must be updated in an atomic way in order to always be consistent. In case of an interruption or incident during the OS Update operation, the OS Developer may choose to implement any technical behaviour, provided that the TOE remains in a secure state. For example, behaviours can be cancelling the operation (the TOE remains the Initial TOE), or entering an error state. The purpose is always to keep consistency between the TOE code and the ID data.

The ST writer shall describe the “secure state” to which the OS update might lead.

18.5 Security Requirements Rationale

Table 18-4: Security Requirements Rationale of OS Update PP-Module

Security Objectives	SFRs	Rationale
O.SECURE_LOAD_ACODE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-VER	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code. FCS_COP.1/OS-UPDATE-VER specifies the cryptographic algorithms used to perform digital signature verification of the additional code to be loaded.

Security Objectives	SFRs	Rationale
O.SECURE_AC_ACTIVATION	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code.
O.TOE_IDENTIFICATION	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FIA_ATD.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FIA_ATD.1/OS-UPDATE maintains the additional code ID for each activated additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code.
O.CONFID-OS-UPDATE.LOAD	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code. FTP_TRP.1/OS-UPDATE provides a trusted path during the transmission of the additional code to the TOE for loading. FCS_COP.1/OS-UPDATE-DEC specifies the cryptographic algorithms used to decrypt the additional code prior to installation.

18.6 SFR Dependencies

Table 18-5: SFR Dependencies of OS Update PP-Module

SFRs	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/OS-UPDATE	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1/OS-UPDATE
FDP_ACF.1/OS-UPDATE	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/OS-UPDATE FMT_MSA.3/OS-UPDATE
FIA_ATD.1/OS-UPDATE	No Dependencies	No Dependencies
FMT_MSA.3/OS-UPDATE	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_SMR.1/OS-UPDATE
FMT_SMR.1/OS-UPDATE	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FMT_SMF.1/OS-UPDATE	No Dependencies	No Dependencies
FTP_TRP.1/OS-UPDATE	No Dependencies	No Dependencies
FCS_COP.1/OS-UPDATE-DEC	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2/GP-ELF FCS_CKM.4 (from [PP-JC])
FCS_COP.1/OS-UPDATE-VER	(FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 (from [PP-JC])

The dependency FMT_MSA.1 of FMT_MSA.3/OS-UPDATE is discarded as no history information has to be kept by the TOE.

Dependencies [FDP_ITC.1 or FCS_CKM.1] of FCS_COP.1/OS-UPDATE-DEC and FCS_COP.1/OS-UPDATE-VER are discarded as the OS Developer is not mandated to rely on GlobalPlatform mechanisms and is free to implement any proprietary solution, provided that the security requirements contained in this PP are met. If necessary, the ST author may add those requirements to the ST.

18.7 Consistency Rationale

The OS Update PP-Module is consistent with the core SE PP and packages:

- The TOE type defined in the PP-Module is based on the TOE type defined in the core PP and packages.

- There are additional threats and OSPs in the PP-Module which do not contradict the core PP and packages.
- There are two new assumptions in the PP-Module related to the extended scope, therefore this does not weaken the core PP and packages.
- There are additional objectives for the TOE, which do not contradict or invalidate the objectives of the core PP and packages.
- There are additional objectives for the environment, which do not weaken the core PP and packages since these are related to the extended scope.
- There are additional SFRs, which do not contradict or invalidate the SFRs of the core PP and packages.