GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
Secure Element Protection Profile
Version 0.0.0.21 (Target v1.0)

Public Review

January 2020

Document Reference: GPC_SPE_174

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
Recipients of this document are invited to submit, with their comments, notification of any relevant patents or other intellectual property rights (collectively, "IPR") of which they may be aware which might be necessarily infringed by the implementation of the specification or other work product set forth in this document, and to provide supporting documentation. This document is currently in draft form, and the technology provided or described herein may be subject to updates, revisions, extensions, review, and enhancement by GlobalPlatform or its Committees or Working Groups. Prior to publication of this document by GlobalPlatform, neither Members nor third parties have any right to use this document for anything other than review and study purposes. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.

The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Contents

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Figures

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Tables

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 and Amendments ([GPCS et al.]). Typical SE form factors include smartcard, eUICC, and eSE.

The core SE 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.]. In particular:

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

Further, the core SE PP defines in Chapters 8-13 six functional packages that address some of the GlobalPlatform’s privileges. These privileges are optionally assigned to the various Security Domains 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 SE PP.

Four PP-Modules defined in Chapters 14-17 of this document 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. This PP-Module is mandatory for SEs with such capability.

The core SE 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 on top of a certified IC conformant with [PP-0084], or on top of a certified Java Card System conformant with [PP-JC].

The core SE 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 core SE PP (including the packages) and any subset of PP-Modules.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

1.1 Identification

1.1.1 SE PP Identification

Title	Secure Element Protection Profile
Reference	GPC_SPE_174
Editor	
Date	
Version	
Sponsor	GlobalPlatform
Author	
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	
Base PP	SE PP, ref GPC_SPE_174
Editor	
Date	
Version	
Sponsor	GlobalPlatform
Author	
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	Contactless Services (CTL) PP-Module
Reference	
Base PP	SE PP, ref GPC_SPE_174
Editor	
Date	
Version	
Sponsor	GlobalPlatform
Author	
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Title	Executable Load File Upgrade (ELFU) PP-Module
Reference	
Base PP	SE PP, ref GPC_SPE_174
Editor	
Date	
Version	
Sponsor	GlobalPlatform
Author	
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	Secure Element Management Services (SEMS) PP-Module
Reference	
Base PP	SE PP, ref GPC_SPE_174
Editor	
Date	
Version	
Sponsor	GlobalPlatform
Author	
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Title	OS Update PP-Module
Reference	
Base PP	SE PP, ref GPC_SPE_174
Editor	
Date	
Version	
Sponsor	GlobalPlatform
Author	
CC Version	3.1 Revision 5
Assurance Level	EAL4 + (ALC_DVS.2, AVA_VAN.5)

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any 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.

Editor’s note: The list of references will be checked prior to publication to keep only the referenced documents.

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.]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Standard / Specification	Description	Ref
GlobalPlatform Card Specification	GlobalPlatform Technology Card Specification v2.3.1, March 2018 Document Reference: GPC_SPE_034	[GPCS]
GPCS Amendment A	GlobalPlatform Card Confidential Card Content Management Card Specification v2.3 – Amendment A v1.1 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 Document Reference: GPC_SPE_011	[Amd B]
GPCS Amendment C	GlobalPlatform Card Technology Contactless Services Card Specification v2.3 – Amendment C v1.2 Document Reference: GPC_SPE_025	[Amd C]
GPCS Amendment D	GlobalPlatform Card Technology Secure Channel Protocol '03' Card Specification v2.3 – Amendment D v1.1.1 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 Document Reference: GPC_SPE_042	[Amd E]
GPCS Amendment F	GlobalPlatform Card Secure Channel Protocol '11' Card Specification v2.3 – Amendment F v1.1 Document Reference: GPC_SPE_093	[Amd F]
GPCS Amendment G	GlobalPlatform Opacity Secure Channel Card Specification v2.3 – Amendment G v1.0 Document Reference: GPC_SPE_106	[Amd G]
GPCS Amendment H	GlobalPlatform Card Executable Load File Upgrade Card Specification v2.3 – Amendment H v1.0 Document Reference: GPC_SPE_120	[Amd H]
GPCS Amendment I	GlobalPlatform Technology Secure Element Management Service Card Specification v2.3 – Amendment I v1.0 Document Reference: GPC_SPE_121	[Amd I]
GP Common Implementation Configuration	GlobalPlatform Card Common Implementation Configuration v2.1, July 2018 Document Reference: GPC_GUI_080	[GP CIC]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Standard / Specification	Description	Ref
GP Composition Model	GlobalPlatform Card Composition Model v1.1, July 2012 Document Reference: GPC_SPE_031	[GP Comp]
GP Composition Guidelines	GlobalPlatform Card Composition Model Security Guidelines for Basic Applications v2.0, Dec 2014 Document Reference: GPC_GUI_050	[GP Comp G]
GP Consumer Configuration	GlobalPlatform Card Technology Consumer-Centric Model Configuration v1.0 Document Reference: GPC_GUI_096	[GP CMC]
GP Contactless Extension Configuration	GlobalPlatform Card Contactless Extension v2.0 Document Reference: GPC_GUI_035	[GP CL Extn]
GP Enhanced ID Configuration	GlobalPlatform Card Technology Privacy Enhanced ID Configuration – PACE/GAP v1.0 Document Reference: GPC_GUI_128	[GP PEIDC]
GP Lifecycle	GlobalPlatform Card Overview of Complete Lifecycle for GP SE Products v1.1, March 2017 Document Reference: GPC_GUI_084	[GP LC]
GP Privacy Framework	GlobalPlatform Card Technology Card Specification – Privacy Framework v1.0, February 2017 Document Reference: GPC_SPE_100	[GP PF]
GP UICC Configuration	GlobalPlatform UICC Configuration v2.0 Document Reference: GPC_GUI_010	[GP UICC]
Cryptographic Algorithm Recommendations	GlobalPlatform Technology Cryptographic Algorithm Recommendations v1.0 Document Reference: GP_TEN_053	[GP Crypto]
Java Card PP	PP0099b – Java Card System – Open Configuration Protection Profile v3.0.5, December 2017	[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]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Standard / Specification	Description	Ref
CEM	Common Criteria for information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1 revision 5	[CEM]
CC Composite	Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018	[CC-Comp]
ANSI X9.52	Triple Data Encryption Algorithm Modes of Operation, draft, 1996	[ANSI X9.52]
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]
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]
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 (TC SCP), 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 (TC SCP), 2004	[TS 102 226]
FIPS PUB 140-2	Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules	[FIPS 140-2]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Standard / Specification	Description	Ref
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]
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 7816-4:2013	Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange	[ISO 7816-4]
ISO/IEC 9797-1	Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher	[ISO 9797-1]
ISO/IEC 10116	Information technology – Modes of operation of an n-bit block cipher algorithm	[ISO 10116]
ISO/IEC 10118-3	Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions	[ISO 10118-3]
ISO/IEC 14888-3:2018	Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms	[ISO 14888]
ISO/IEC 19772/AC1:2014	Information technology – Security techniques – Authenticated encryption [ISO/IEC 19772:2009 with Technical correction]	[ISO 19772]
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 800-56C	Recommendation for Key Derivation through Extraction-then-Expansion. November 2011	[NIST 800-56C]
NIST SP 800-57 Part 1 Revision 3	Recommendation for Key Management – Part 1: General (Revision 3), July 2013.	[NIST 800-57]
NIST SP 800-73-4	Interfaces for Personal Identity Verification – May 2015	[NIST 800-73-4]
NIST SP 800-90A	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012	[NIST 800-90A]
NIST SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009.	[NIST 800-108]
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	[RFC 2119]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Standard / Specification	Description	Ref
RFC 2246	The TLS Protocol – Version 1.0	[TLS 1.0]
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 4346	The TLS Protocol – Version 1.1	[TLS 1.1]
RFC 4366	Transport Layer Security (TLS) Extensions	[TLS Extns]
RFC 4785	Pre-Shared Key (PSK) Cipher Suites with NULL Encryption for Transport Layer Security (TLS)	[PSK NULL]
RFC 5246	The TLS Protocol – Version 1.2	[TLS 1.2]
RFC 5487	Pre-Shared Key Cipher Suites for TLS with SHA-256/384	[PSK 256]
RFC 5639	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation	[RFC 5639]
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, v3.0.5 Classic Edition, May 2015	[JCAPI]
Java Card VM	Virtual Machine Specification, Java Card™ Platform, v3.0.5 Classic Edition, May 2015	[JCVM]
Java Card JCRE	Runtime Environment Specification, Java Card™ Platform, v3.0.5 Classic Edition, May 2015	[JCRE]

1.5 Terminology and Definitions

The following meanings apply to SHALL, SHALL NOT, MUST, MUST NOT, SHOULD, SHOULD NOT, and MAY in this document (refer to [RFC 2119]):

- **SHALL** indicates an absolute requirement, as does **MUST**.
- **SHALL NOT** indicates an absolute prohibition, as does **MUST NOT**.
- **SHOULD** and **SHOULD NOT** indicate recommendations.
- **MAY** indicates an option.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

Editor’s note: The list of terms will be checked prior to publication to comply with the latest approved GlobalPlatform definitions and to keep only the terms that are effectively used.

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 uses two related transformations, a public transformation (defined by the Public Key component) and a private transformation (defined by the Private Key component); these two key components have a property so that it is computationally infeasible to discover the Private Key, even if given the Public Key.
Basic Logical Channel	The permanently available interface between the card and an external entity. The Basic Logical Channel is numbered zero.
Card Content	Code and Application information (but not Application data) contained in the card that is under the responsibility of the OPEN; e.g. Executable Load Files, Application instances, etc.
Card Image Number (CIN)	An identifier for a specific GlobalPlatform card.
Card 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Term	Definition
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.
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 and 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).

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Term	Definition
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.
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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Term	Definition
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.
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 (SCP)	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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Term	Definition
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 some undefined mechanism such as a secure process that delivers the public key in a self-signed certificate. A Trust Point's public key is typically the 'highest' public key known to the entity.
UICC	In the context of this document, the UICC as defined by ETSI Project Smart Card Platform (EP SCP) 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
0 - 9	Decimal digits are not enclosed in quotation marks.
'0' - '9' and 'A' - 'F'	Hexadecimal values are enclosed in straight single quotation marks.
AES	Advanced Encryption Standard
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
CIN	Card Image Number
CL	Contactless

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Abbreviation / Notation	Meaning
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
KID	Key Identifier
KVN	Key Version Number
MAC	Message Authentication Code
MNO	Mobile Network Operator
NA	Not Applicable
OE	Operational Environment
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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Abbreviation / Notation	Meaning
SCP	Secure Channel Protocol or Smart Card Platform
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; see Table 1-3
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
Dec 2018	0.0.0.8	Committee Review
October 2019	0.0.0.14	Member Review
January 2020	0.0.0.21	Public Review
TBD	1.0	Public Release

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

2 TOE Overview

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

2.1 TOE Type

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

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

The TOE is composed of the following components:

- IC and Dedicated Software certified against [PP-0084]
- Java Card System comprised of the runtime environment (JCRE), virtual machine (JCVM) and API (JCAPI). Native code may complete this layer. This may be certified according to [PP-JC].
- GlobalPlatform Card Framework as a set of items covering the Card Manager (OPEN), Trusted Framework, GlobalPlatform APIs and ISD. Note that the pre-issuance SD(s) are optional, e.g. APSD(s) and CASD(s).

The TOE user security guidance is part of the TOE.

The TOE does not comprise the Applicative Security Domains and Applications.

The SE PP extends the Java Card PP Open Configuration [PP-JC] with security requirements for the GlobalPlatform Card Framework of the TOE. Following the approach used in the Java Card PP, the SE PP defines additional security problems, objectives and requirements for the SE Platform composed of the Java Card System and the GlobalPlatform Card Framework, and covers the IC and Dedicated Software through security objectives for the environment, which become objectives for the TOE in a conformant Security Target (ST).

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 OS update is addressed here, not OS replacement.

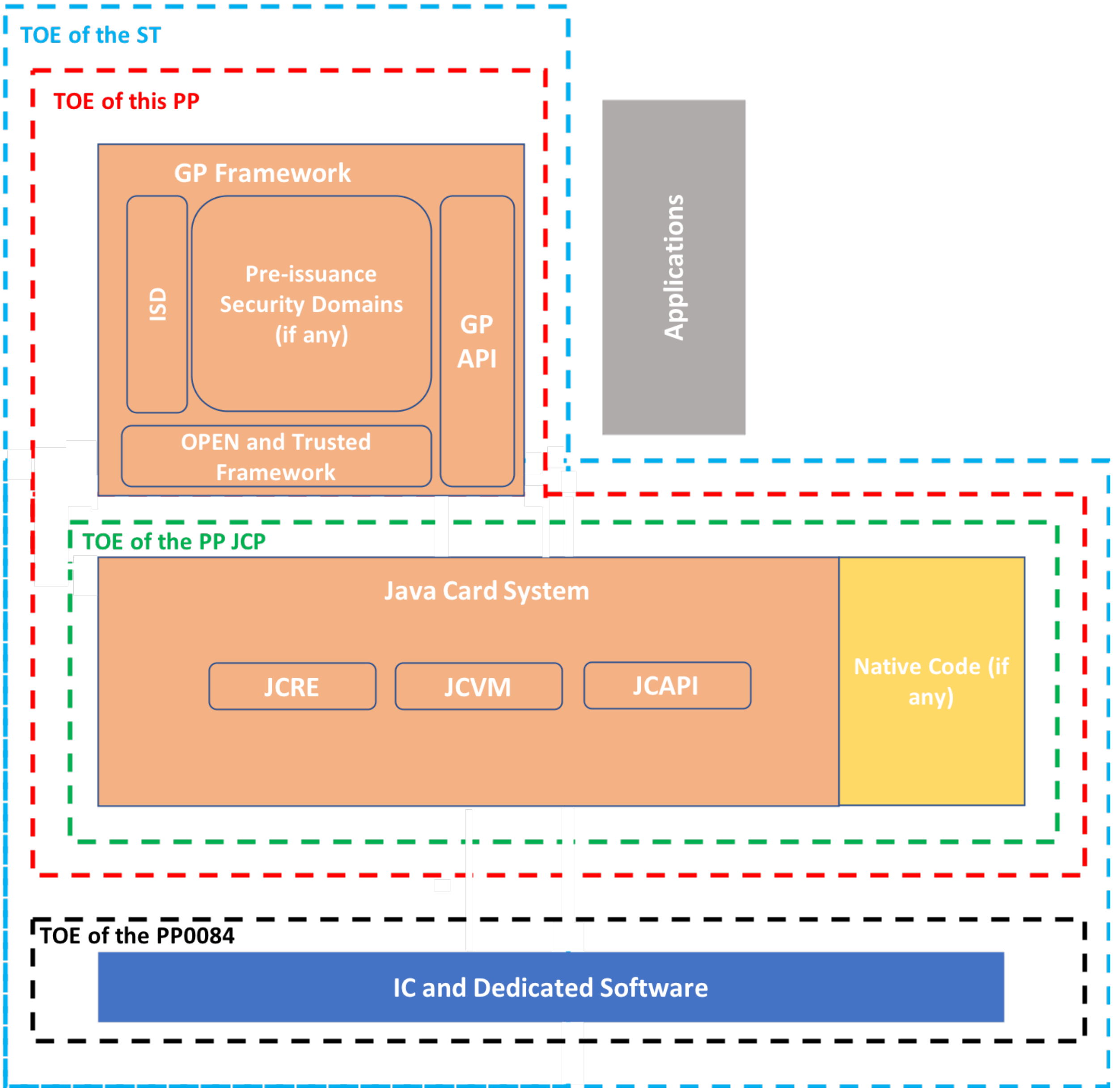
2.2 TOE Description

Figure 2-1 illustrates the common architecture of the TOE.

- The red dashed line shows the TOE under the scope of the SE PP. The TOE includes the Java Card System and the GlobalPlatform Card Framework.
- The scope of an SE evaluation conformant to this PP is represented by the blue dashed line.
- Post-issuance Applications and SD(s) are out of scope.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Figure 2-1: TOE Components



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

2.2.1 GlobalPlatform Functionalities

The GlobalPlatform Card 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 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 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- GlobalPlatform Environment (OPEN) provides an API to applications, command dispatch, Application selection, (optional) logical channel management, and card content management. 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), which provides the on-card bytecode interpreter.
- The Java Card Runtime Environment (JCRE), which is responsible for resource management, isolation between applets, communication, applet execution, and applet security.
- The Java Card Application Programming Interface (JCAPI), which 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, PIN and cryptographic specific management and the exceptions mechanism.

2.3 Major Security Features of the TOE

The main security features of 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 Card 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 Card 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) that is verified on card by the on-card representative of the VA prior to the 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).

[1] Note that as in Java Card PP, this PP assumes that all the bytecodes are verified at least once before loading, installation, or execution.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- 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 keysets 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 SD keysets creation and personalisation of the Application Provider Security Domain (APSD) [Amd A]. These keysets are not known by the Issuer.
- 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 being transmitted but can only apply to the environment and/or context in which 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 SE PP as illustrated in Table 2-1.

The SE PP does not prescribe the use of one SCP or another; the choice of the SCP and cryptographic algorithms for secure communication is specific to the Issuer and Service Providers.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 3DES in CBC mode with fixed IV of binary zeros therefore its encryption scheme is deterministic and not highly secure and thus vulnerable to a classical plaintext-recovery attacks. SCP02 is deprecated in GlobalPlatform Card Specification v2.3.1. Use of another Secure Channel Protocol, such as Secure Channel Protocol '03' (SCP03), is recommended.
SCP03	[Amd D]	AES	SCP03 uses Advanced Encryption Standard (AES) encryption algorithm with randomly generated Initialization vector (IV) and hence its encryption scheme is un-deterministic and highly secure. SCP03 provides strong security guarantees, resistance to 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) and secure messaging protection of commands and responses using symmetric cryptography.
SCP11	[Amd F]	ECC	SCP11 offers authentication services using an ECC-based Public Key Infrastructure (PKI) and 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]).
SCP22	[Amd G]	ECC + Opacity	SCP22 is the Opacity Secure Channel establishment methods which includes Opacity ZKM, FS, and Blinded protocols.
SCP80	[TS 102 225] and [TS 102 226]	AES/DES	SCP80 supports the Over-The-Air security scheme defined in [TS 102 225] and [TS 102 226]. Note: As DES is not highly secure and thus vulnerable to a classical plaintext-recovery attacks, use of AES is recommended.
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. Note: Use of TLS version 1.2 is recommended.

2.3.3 Cryptographic Operations

The types of cryptographic operations to be supported by the SE are the following:

- Symmetric Encryption/Decryption (TDES, AES)
- Asymmetric Encryption/Decryption (RSA, ECC)
- Signature generation and verification (RSA, ECDSA)

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- MACing (R-MAC, C-MAC)
- Random Number Generation
- Key Generation
- Key Derivation (DES, AES)
- 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:

In the core SE 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-ENC FCS_COP.1/SEMS-MAC FCS_COP.1/SEMS-SIG-VER
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 contexts to provide tamper-resistant data and execution protection, for instance:

- Financial applications, like credit/debit/pre-paid cards
- Transport and ticketing, e.g. granting pre-paid access to a transport system
- Telephony, through the Subscriber Identification Module (SIM) or NFC chips or eUICC
- Personal identification/authentication
- Electronic passport and identity card
- Secure information storage, like health records or health insurance cards

2.5 Available Non-TOE Hardware/Software/Firmware

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

- Bytecode Verifier
- 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

2.6 TOE Life Cycle

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

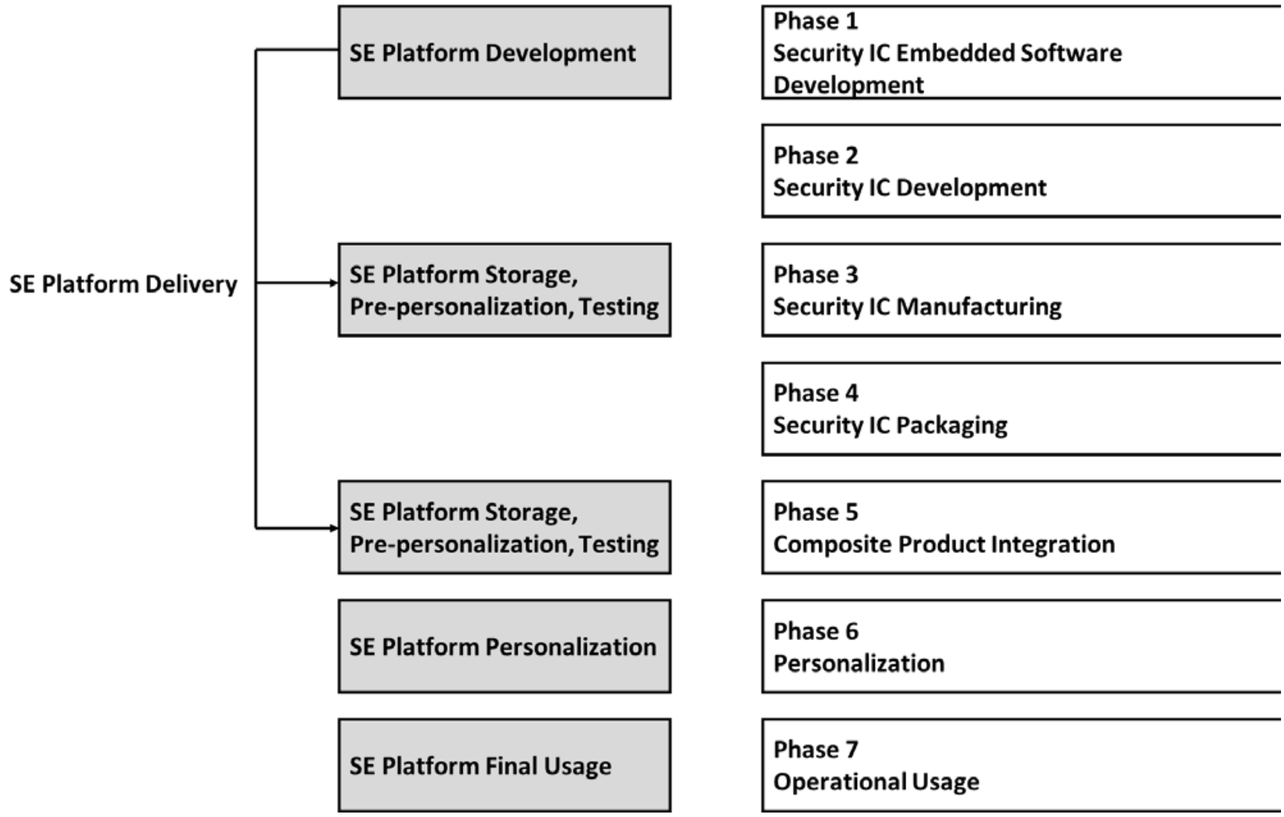
- Phases 1 and 2 compose the product development: IC and Embedded Software (IC Dedicated Software, Java Card System, GlobalPlatform Card Framework, SDs, Applications) development.
- Phase 3 and Phase 4 correspond to IC manufacturing and packaging, respectively. Some IC pre-personalisation steps may occur in Phase 3.
- 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


SE Platform Delivery
SE Platform Development
SE Platform Storage, Pre-personalization, Testing
SE Platform Storage, Pre-personalization, Testing
SE Platform Personalization
SE Platform Final Usage
Phase 1 Security IC Embedded Software Development
Phase 2 Security IC Development
Phase 3 Security IC Manufacturing
Phase 4 Security IC Packaging
Phase 5 Composite Product Integration
Phase 6 Personalization
Phase 7 Operational Usage

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

TOE Development is performed during Phase 1. This includes the Java Card System and the GlobalPlatform Card Framework conception, design, implementation, testing, and documentation. The TOE development shall fulfil requirements of the final product, including conformance to functional specifications (if applicable) and recommendations of the IC user guidance. The TOE development shall occur in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees 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 Security IC Manufacturing (Phase 3) or during Composite Product Integration (Phase 5). It is also possible that 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. TOE delivery shall usually involve encrypted signed sending and it supposes the previous 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. If the Security IC has already been certified (e.g. 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) TOE storage in Phase 5 implies a product delivery after Phase 5. Hence, the evaluation of such product against this PP shall include the Composite Product Integrator environment (may be more than one if there are many integrators).

The TOE is personalised in Phase 6, if necessary. The Personalisation environment shall be included in a product evaluation only if the product delivery point is at the end of Phase 6. This means that some of the product personalisation operations may require a controlled environment (secure locations, secure procedures and trusted personnel). The product shall be tested again and 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 TOE final usage environment is that of the product where the TOE is embedded in. 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 applications loading and personalisation) can occur during production in a secure 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, 5, or 6 depending on the product itself. Note that TOE delivery precedes product delivery. During product evaluation against this Protection Profile, the ALC security assurance requirements apply to the whole product life cycle up to delivery.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

2.7 Actors of the TOE

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

- **Issuer** (e.g. MNO or bank), owner of the TOE. The TOE guarantees that the Issuer, once authenticated, can manage the loading, instantiation and deletion of Applications.
- **Application Provider (AP)**, entity or institution responsible for the Applications and their associated services.
- **Controlling Authority (CA)**, entity independent from the Issuer and responsible for providing on card security services such as confidential key loading, signatures and Mandated DAP.
- **Verification Authority (VA)**, a Controlling Authority whose responsibility is to enforce control over card contents 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 author shall indicate the functional packages and PP-Modules to which the ST claims conformance.

The table below 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.

The ST author shall:

- Indicate if SSDs are supported (YES or NO).
- Complete the table (? cells) for all the privileges that are effectively supported by the implementation (YES or NO) 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 CCCM ([Amd A]) and ELFU ([Amd H]) are not linked to any privilege.
- Select the PP-Modules that are not linked to privileges (ELFU, CCCM, and 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 features (M) and optional features effectively implemented by the TOE (YES).

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

3 Conformance Claims and Consistency Rationale

3.1 CC Conformance Claims

The core SE PP, functional packages, and PP-Modules claim conformance to:

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

The core SE PP and PP-Modules claim conformance to:

- CC Part 3 [CC3]

3.2 Conformance Claim to a Package

The core SE PP and PP-Modules claim 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

The core SE PP is conformant to the Java Card System Open Configuration Protection Profile [PP-JC].

Several concepts and definitions given in this Protection Profile come from the USIM PP [USIM PP]; nevertheless, this PP does not claim conformance to the USIM PP.[2]

3.4 Conformance Claim to the PP

The core SE PP and PP-Modules require demonstrable conformance (as defined in [CC1]) of any conformant 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 in the core SE PP extends the Java Card System defined in [PP-JC].

[2] The USIM PP answers the problem of card management in the context of MNOs. Unlike USIM PP, the SE PP is generic.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

3.5.2 SPD Consistency

3.5.2.1 Assets

All the assets defined in [PP-JC] are relevant for the TOE of the core SE PP.

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	R
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 [PP-JC].

3.5.2.2 Users and Subjects

All the subjects defined in [PP-JC] are relevant for the TOE of the core SE PP.

The table below indicates the subjects' consistency statement.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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.PACKAGE	x	E
S.SD		A
S.OPEN		A

3.5.2.3 Threats

All the threats defined in [PP-JC] are relevant for the TOE of the core SE PP.

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
T.NATIVE	x	E

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

T.UNAUTHORISED-CARD-MNGT refines T.INSTALL and T.DELETION from [PP-JC].

T.DELETION replaces A.DELETION from [PP-JC].

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)

All the OSPs defined in [PP-JC] are relevant for the TOE of the core SE PP.

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.OTA-LOADING		A
OSP.OTA-SERVERS		A
OSP.APSD-KEYS		A
OSP.KEY-GENERATION		A
OSP.CASD-KEYS		A
OSP.KEY-CHANGE		A
OSP.SECURITY-DOMAINS		A
OSP.ISSUER-KEYS		A
OSP.APPLICATIONS		A

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

3.5.2.5 Assumptions

All the assumptions defined in [PP-JC] are relevant for the TOE in the core SE PP except A.DELETION that is replaced by O.DELETION.

The table below provides the assumptions' consistency statement.

Table 3-5: Assumptions Consistency Statement

Assumptions	[PP-JC]	Core SE PP
A.APPLET	x	E
A.VERIFICATION	x	E
A.OTA-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

3.5.3 Security Objectives Consistency Statement

The entire set of objectives for the TOE and for the environment that are defined in [PP-JC] are relevant for the TOE of the core SE PP.

3.5.3.1 Security Objectives for the TOE

The table below provides consistency statement for the '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.NATIVE	x	E
O.OPERATE	x	E
O.REALLOCATION	x	E

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Objectives for the TOE	[PP-JC]	Core SE PP
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

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.APPLET	x	E
OE.CARD-MANAGEMENT	x	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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Objectives for the Environment	[PP-JC]	Core SE PP
OE.OTA-ADMIN		A
OE.APPS-PROVIDER		A
OE.VERIFICATION-AUTHORITY		A
OE.KEY-ESCROW		A
OE.PERSONALISER		A
OE.CONTROLLING-AUTHORITY		A
OE.PRODUCTION		A
OE.AID-MANAGEMENT		A
OE.OTA-LOADING		A
OE.OTA-SERVERS		A
OE.AP-KEYS		A
OE.KEY-GENERATION		A
OE.CA-KEYS		A
OE.VA-KEYS		A
OE.KEY-CHANGE		A
OE.SECURITY-DOMAINS		A
OE.ISSUER		A
OE.ISSUER-KEYS		A
OE.APPLICATIONS		A

OE.CARD-MANAGEMENT defined in [PP-JC] becomes an objective for the TOE in the core SE PP.

3.5.4 SFRs and SARs Consistency Statements

3.5.4.1 Consistency of Policies

All the security policies of [PP-JC] are relevant to the TOE of the core SE 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 SD/Application keys and data through STORE DATA and PUT KEY commands.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

3.5.4.2 Consistency of SFRs

All the mandatory SFRs of [PP-JC] are relevant to the TOE of the core SE PP as shown in the table below.

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
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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SFRs	[PP-JC]	Core SE PP
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)
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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SFRs	[PP-JC]	Core SE PP
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
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 SARs’ Consistency

The core SE PP claims the same evaluation assurance level as [PP-JC], that is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 unless the asset is refined.

4.1.1 User Data

Table 4-1: User Data Assets Refined from [PP-JC]

D.APP_I_DATA	Integrity sensitive data of the applications, like the data contained in an object, a static field of a package, a local variable of the currently executed method, the CVM security attributes (such as CVM value, CVM State, CVM Retry Limit, and CVM Retry Counter), or a position of the operand stack. To be protected from unauthorised modification.

Table 4-2: 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

4.1.2 TSF Data

Table 4-3: Additional TSF Data Assets Related to [GPCS]

D.GP_REGISTRY	The information resource for Card Content management. The GP 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 4-4: 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 GP Environment (OPEN) on the card. The main responsibilities 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 SE PP adds specific threats related to Card Management and Secure Communication as defined in the specification [GPCS].

4.3.1 Java Card System

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

4.3.2 Card Management

Table 4-5: Additional Threats for Card Management

T.UNAUTHORISED-CARD-MNGT	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, 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	An attacker accesses to 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 4-6: Additional Threats for Secure Communication

T.COM-EXPLOIT	An attacker remotely exploits the communication channels established between a third party and the TOE in order to modify or disclose confidential data. All assets are threatened.
T.BRUTE-FORCE-SCP	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. All assets are threatened.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 4-7: 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.OTA-LOADING	Application code, validated or certified depending on the application, is loaded "Over the Air" (OTA) onto the SE Platform using OTA servers. If needed, the Issuer can pre-authorise content loading operation through delegated management privilege to 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.OTA-SERVERS	A security policy shall be employed by the Issuer to ensure the security of the applications stored on its servers.
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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 4-8: Additional Assumptions Related to [GPCS]

A.ISSUER	Entity that owns the SE and is ultimately responsible for the behaviour of the SE.
A.OTA-ADMIN	Administrators of the OTA servers or any other server used to perform card content management are trusted actors. They are trained to use and administrate securely those servers. 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 to the administration of OTA servers.
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 who is able to guarantee and check the digital signature attached to 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 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	If the TOE delivery occurs before Phase 6 of the SE life cycle, then production and personalisation environment is trusted and secure.
A.SCP-SUPP	The operational environment supports and uses the SCPs offered by the TOE.
A.KEYS-PROT	The keys which are stored outside the TOE and which are used for secure communication and authentication between SE and external entities are protected for confidentiality and integrity in their own storage environment. This covers D.APSD_KEYS and D.ISD_KEYS.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 card manager as defined in [GPCS] section 3.8 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. This component will in practice be tightly connected with the TOE, which in turn shall very likely rely on the card manager for the effective enforcing of some of its security functions. 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 should prevent card content management operations (loading, installation, deletion) from being carried out, for instance, at invalid states of the card or by non-authorised actors. It shall also enforce security policies established by the Issuer.
O.DOMAIN-RIGHTS	The Issuer shall not get access or change personalised APSD keys, which belong exclusively to the AP. Modification of an SD key set is restricted to the AP who owns the SD.
O.APPLI-AUTH	The card manager shall enforce the application security policies established by the Issuer 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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.OTA-ADMIN	Administrators of the OTA servers shall be trusted actors. They shall be trained to use and administrate those servers. They have the means and the equipment’s to perform their tasks. They must be aware of the sensitivity of the assets they manage and the responsibilities associated to the administration of OTA servers.
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 who is able to guarantee and check 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

OE.PERSONALISER	The personaliser shall be a trusted actor in charge of the personalisation process. The personaliser must ensure the security of the keys it manages and loads 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 their own keys by operational means and/or procedures.

5.2.3 Secure Places

Table 5-5: Additional OEs for Secure Places

OE.PRODUCTION	Production and personalisation environments, if the TOE delivery occurs before Phase 6 of the life cycle, must be trusted and secure.

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.OTA-LOADING	Application code, validated or certified depending on the application, is loaded "Over-The-Air" (OTA) onto the SE Platform using OTA servers. This process should protect the confidentiality and the integrity of the loaded application code.
OE.OTA-SERVERS	The Issuer must enforce a policy to ensure the security of the applications stored on its servers.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

5.2.6 Keys

Table 5-8: Additional OEs for Keys

OE.AP-KEYS	The SD keys personaliser, the AP and the key escrow must enforce a security policy on SD keys in order to secure their transmission.
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 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 from disclosing encrypted data transiting to the card.

T.UNAUTHORISED-CARD-MNGT 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 from disclosing encrypted data transiting to the card.
- O.APPLI-AUTH requires for loading all applications to be authenticated.
- O.DOMAIN-RIGHTS restricts the modification of an AP security domain keyset to the AP who owns 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 that controls the access to card management functions such as the loading, installation, extradition, or deletion of applets and prevent attacks intended to modify or exploit the current life cycle of applications.
- O.DOMAIN-RIGHTS that restricts the use of an AP security domain keysets, and thus the management of the applications related to this SD, to the AP who owns it.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

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

5.3.3 Assumptions

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

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

5.3.4 Rationale Tables of SPD and Security Objectives

Table 5-9: Threats and Security Objectives

SPDs	Security Objectives
T.COM-EXPLOIT	O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
T.UNAUTHORISED-CARD-MNGT	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.OTA-LOADING	OE.OTA-LOADING
OSP.OTA-SERVERS	OE.OTA-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	OE.SECURITY-DOMAINS
OSP.APPLICATIONS	OE.APPLICATIONS
A.ISSUER	OE.ISSUER
A.OTA-ADMIN	OE.OTA-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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

6 Extended Requirements

6.1 Extended Families

6.1.1 Extended Family FCS_RNG – Generation of Random Numbers

6.1.1.1 Description

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.

6.1.1.2 Extended Components

Extended Component FCS_RNG.1

Description

Generation of random numbers requires that random numbers meet a defined quality metric.

Hierarchical to: No other components.

Management: No management activities are foreseen.

Audit: No actions are defined to be auditable.

Definition

FCS_RNG.1 Random numbers generation

FCS_RNG.1.1 The TSF shall provide a **[selection: physical, non-physical true, deterministic, hybrid, hybrid deterministic]** random number generator that implements: **[assignment: list of security capabilities]**.

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

Dependencies: No dependencies.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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); the other group of SFRs is new and covers GlobalPlatform specifications [GPCS] (see subsections of section 7.1.2).

The set of underlying security functional policies is the following:

[PP-JC] (see section 7.1.1)	SE PP (see section 7.1.2)	Description
Firewall access control SFP		Included in SE PP by reference
ADEL access control SFP		Included in SE PP by reference
JCVM information flow control SFP		Included in SE 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

All the SFRs of the [PP-JC] are relevant to the TOE of the core SE PP. These SFRs are not duplicated here. The ST author must refer to the [PP-JC] to build the ST.

All the SFRs with suffix /CM and /Installer defined in [PP-JC] are replaced by more specific and detailed requirements in the 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. No additional requirements are needed.

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)

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- /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, GP 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 Executable Load File 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]**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 Executable Load Files**
- **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 belongs 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 and 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'.

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: 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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:

- **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, the major (minor) Version attribute associated to the dependent ELF is less than or equal to the major (minor) Version attribute associated to 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, [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: GP APDU commands STORE DATA and PUT KEY, GP 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:

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- **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).**
- **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 being forwarded 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 belong 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 belongs to the policy 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 and 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’.

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: 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 Card**
- **[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]**.

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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’.

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]**.

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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

7.1.2.5 Secure Communication

The purpose of a Secure Channel Protocol (SCP) is to authenticate the on-card and off-card entities and to allow the protection of the data exchanged between them, for Authenticity, Integrity, and Confidentiality.

The Secure Communication requirements cover all the 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, altogether 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 that belong 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 ([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]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

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 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 to generate an ephemeral EC key pair. Recommendations for appropriate random number generators are given in BSI TR-02102 [TR 02102], NIST SP 800-90A [NIST 800-90A] and ANSSI's RGS [ANSSI-RGS].

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 **the session 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 selected cryptographic operations from the table below]** in accordance with a specified cryptographic algorithm **[assignment: list of cryptographic algorithms from the table below]** and cryptographic key sizes **[assignment: list of cryptographic key sizes from the table below]** that meet the following: **[assignment: list of standards from the table below]**

SCP Protocol	Operation	Algorithm	Length	Recommended Standards
SCP02	MAC Generation/Verification	R-MAC TDES	112 bits	[ISO 9797-1]
SCP02	Symmetric Encryption/Decryption	TDES in CBC mode	112 bits	[ANSI X9.52] and [ISO 10116]
SCP02	Symmetric Encryption/Decryption	TDES in ECB mode	112 bits	[ANSI X9.52] and [ISO 10116]

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SCP Protocol	Operation	Algorithm	Length	Recommended Standards
SCP03, SCP11	Symmetric Encryption/Decryption	AES in CBC mode	128, 192, or 256 bits	[FIPS 197], [NIST 800-38A], and [FIPS 140-2]
SCP10	Asymmetric Encryption/Decryption	RSAES-PKCS1-v1_5, RSAES-OAEP	>1024 bits	[PKCS#1]
SCP22	Authenticated Encryption (AEAD)	AES	128, 192, or 256 bits	[ISO 19772]
SCP22	Key Derivation	AES	128, 192, or 256 bits	[NIST 800-56A], [NIST 800-56C], [NIST 800-108]
SCP22	Secure Messaging	ECDH : Opacity ZKM and Opacity FS		[ANSI 504-1], [NIST 800-73-4]
SCP22	Asymmetric Encryption/Decryption	ECC	256, 384, 512, 521 bits	[RFC 5639]
SCP22	Digital Signature	RSASSA-PKCS-v1_5 with SHA-1, RSASSA-PSS with SHA-256	>=1024 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]
SCP22	MAC Generation/Verification	CMAC AES	128, 192, or 256 bits	[NIST 800-38B] and [FIPS 140-2]
SCP22	Key Agreement	ECKA		[NIST 800-56A]
SCP22	Key Derivation	ECKA-EG		[TR 03111]
SCP22	Has Computing	SHA-256, SHA-384, SHA-512		[ISO 10118-3] and [FIPS 180-4]
SCP21	Privacy-enable Secure Channel (Prevention of privacy leakage)			[419 212] part 1, [ICAO 9303]
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	PSK TLS		[PSK TLS]
SCP81	Encryption/Decryption	TDES or AES		[PSK TLS]

Application Note:

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

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 GP 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 GP 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].**

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorised Identified Roles with Privileges
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

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	

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]			

Legend:

AM SD: Security Domain with Authorised Management privilege

DM SD: Security Domain with Delegated Management privilege

SD: Other Security Domain

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 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]:**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- **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 (note however that when the list of failures is empty, there is no need to define a maintenance mode), when the list of failures is empty), the second one allows to state which types of failure or service discontinuity require automatic recovery procedures. Examples of failures include interruption of installation of an Executable Load File, interruption of a package/application deletion, loss of 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:

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- **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 belong 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, 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 on 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 GP Registry.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 by the following ones:

O.LOAD, O.INSTALL and O.DELETION are covered by all SFRs as these security objectives specifies that the loading of a package into the card, the installation of applications and the deletion of packages/applications must be secure.

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 for preventing any possible misinterpretation of the Security Domain keys used to implement a Secure Channel when they 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:

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- 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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.

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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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.

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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, they specify the actions that can be performed before authenticating the origin of the APDU commands that the card receives.
- 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 unobservability 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 for preventing any possible misinterpretation of the Security Domain keys used to implement a Secure Channel when they are loaded form 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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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, they specify the actions that can be performed before authenticating the origin of the APDU commands that the card receives.
- 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 transitions. It specifies the actions protecting the card management commands.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.

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

- FDP_ROL.1/GP ensures the rollback of the installation or removal operation on the executable files and application instances.
- 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.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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.

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 roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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, they specify the actions that can be performed before authenticating the origin of the APDU commands that the card receives.
- FCS_COP.1/GP-SCP specifies the cryptographic operations and algorithms that shall be used to ensure the authenticity of the card management commands.
- FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transitions. It specifies the actions protecting the card management 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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- 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 transitions. It specifies the actions protecting the card management 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 transitions. It specifies the actions protecting the card management commands.
- FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the roles Application Provider/Controlling Authority and specifies the authorised identified roles enabling to send and authenticate card management commands for which the integrity, authenticity, and/or confidentiality have to be ensured.
- 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.

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

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

7.3.2 Rationale Tables of Security Objectives and SFRs

Table 7-1: SFRs and Security Objectives

SFR	Security Objectives
FMT_SMR.1/GP	O.FIREWALL, O.RESOURCES, O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.SECURITY-DOMAINS, O.PRIVILEGES-MANAGEMENT, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY, O.SID
FMT_SMF.1/GP	O.SID, O.FIREWALL, O.RESOURCES, O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.SECURITY-DOMAINS, O.PRIVILEGES-MANAGEMENT, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FDP_ROL.1/GP	O.CARD-MANAGEMENT, O.APPLI-AUTH
FCO_NRO.2/GP	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FDP_ITC.2/GP-ELF	O.SID, O.FIREWALL, O.CARD-MANAGEMENT
FDP_ITC.2/GP-KL	O.SID, O.FIREWALL, O.CARD-MANAGEMENT
FPT_FLS.1/GP	O.OPERATE, O.RESOURCES, O.ALARM, O.CARD-MANAGEMENT, O.APPLI-AUTH
FPT_RCV.3/GP	O.OPERATE, O.RESOURCES, O.CARD-MANAGEMENT
FMT_MTD.1/GP-LC	O.LC-MANAGEMENT
FMT_MTD.1/GP-PR	O.PRIVILEGES-MANAGEMENT
FMT_MTD.3/GP	O.PRIVILEGES-MANAGEMENT, O.LC-MANAGEMENT
FDP_IFC.2/GP-ELF	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FDP_IFF.1/GP-ELF	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FIA_UID.1/GP	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH
FIA_AFL.1/GP	O.NO-KEY-REUSE, O.CARD-MANAGEMENT
FIA_UAU.1/GP	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH
FIA_UAU.4/GP	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.NO-KEY-REUSE
FDP_UIT.1/GP	O.CARD-MANAGEMENT
FDP_UCT.1/GP	O.CARD-MANAGEMENT
FTP_ITC.1/GP	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FPR_UNO.1/GP	O.CARD-MANAGEMENT
FPT_TDC.1/GP	O.CARD-MANAGEMENT, O.KEY-MNGT
FCS_CKM.1/GP-SCP	O.CIPHER, O.KEY-MNGT

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SFR	Security Objectives
FCS_COP.1/GP-SCP	O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY, O.CIPHER, O.KEY-MNGT
FCS_RNG.1/GP-SCP	O.RNG
FDP_IFC.2/GP-KL	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FDP_IFF.1/GP-KL	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FMT_MSA.1/GP	O.SID, O.FIREWALL, O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY
FMT_MSA.3/GP	O.SID, O.FIREWALL, O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY

7.3.3 Dependencies

7.3.3.1 SFRs Dependencies

Table 7-2: 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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SFRs	CC Dependencies	Satisfied Dependencies
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
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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SFRs	CC Dependencies	Satisfied 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])
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 7-3: 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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SARs	CC Dependencies	Satisfied Dependencies
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
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. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defence against such attacks: the evaluators should have access to the low-level design and source code. The lowest for which such access is required is EAL4.

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, in particular 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 of them are satisfied 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 may 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 nature of the TOE and embedding product, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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	The attacker discloses a Ciphered Load File Data Block when it is transmitted to the SE for decryption prior to installation. 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

Objectives	Threats, OSP
O.CLFDB-DECIPHER	T.CLFDB-DISC, OSP.CLFDB-ENC-PR
OE.CLFDB-ENC-PR	OSP.CLFDB-ENC-PR

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 **DES with CBC mode, AES with CBC mode with a null ICV** and cryptographic key sizes **16-byte DES, 16-byte, 24-byte, or 32-byte AES** that meet the following: **TDES: [ISO 9797-1], AES: [FIPS 197]**.

Application Note: See [GPCS] section C.6.

8.5 Security Requirements Rationale

SFRs	Objectives
FCS_COP.1/GP-CLFDB	O.CLFDB-DECIPHER

8.6 SFR Dependencies

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)

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

9 Package 'Global Services (GS)'

9.1 Scope

The Package 'GS' is to be considered if the new 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-MNGT from [PP-JC].	

9.3 Objectives

Table 9-2: Objectives of GS Package

Security Objectives for the TOE
O.CARD-MANAGEMENT from [PP-JC].

9.3.1 Security Objectives Rationale

Objectives	Threats
O.CARD-MANAGEMENT	T.UNAUTHORISED-CARD-MNGT

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

9.4 Security Functional Requirements

FDP_ACC.1/GP-GS Subset access control

FDP_ACC.1.1/GP-GS The TSF shall enforce the **GP 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**
  - **GP 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 **GP 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 GP Registry**
  - **AID: Associated or Not associated**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 GP Registry for another on-card entity.**
    - **On receipt of service deregistration request, S.OPEN checks that the requested service name is registered in GP 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

FMT_MSA.1/GP-GS Management of security attributes

FMT_MSA.1.1/GP-GS The TSF shall enforce the **GP 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 **GP 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

SFRs	Objectives
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	O.CARD-MANAGEMENT

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

9.6 SFR Dependencies

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 the version 2.3.1 of the Specification (see [GPCS] section 8.2) there is one CVM standardised by GlobalPlatform: the global Personal Identification Number (Global PIN).

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	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_RETRY_COUNTER	A counter, used in conjunction with the Retry Limit, to determine when attempts to present a CVM value shall be prohibited. To be protected from unauthorised modification.
D.CVM_RETRY_LIMIT	The maximum number of times an invalid CVM value can be presented prior to the CVM handler prohibiting further attempts to present a CVM value. To be protected from unauthorised modification.
Threats	
T.CVM-IMPERSONATE	The attacker may try to impersonate the Cardholder to disclose or guess the PIN stored in CVM in order to gain access to the services that the card offers.
T.CVM-RESET	The attacker executes an application that tries to reset the PIN code of the CVM.
T.BRUTE-FORCE-CVM	APDU commands/API methods can be repeatedly transmitted/invoked to attempt the brute force extraction of secrets such as PINs.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 some privileged applications appointed by the Card Manager. Any SD allowed to perform CVM can grant the CVM privilege to an Application.
O.CVM-BLOCK	No further Cardholder authentication attempts shall be possible once the maximal number of attempts has been reached, until a special action is performed by the Card Manager or by a privileged User.
O.CVM-MNGT	The TOE shall provide a 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

Objectives	Threats, OSP
O.GLOBAL-CVM	T.CVM-IMPERSONATE
O.CVM-BLOCK	T.CVM-IMPERSONATE, T.BRUTE-FORCE-CVM
O.CVM-MNGT	T.CVM-IMPERSONATE, T.CONFID-APPLI-DATA, T.INTEG-APPLI-DATA

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]**.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

10.5 Security Requirements Rationale

SFRs	Objectives
FIA_AFL.1.1/GP-CVM	O.CVM-BLOCK, O.CVM-MNGT
FPR_UNO.1/GP-CVM	O.CVM-MNGT, O.GLOBAL-CVM

10.6 SFR Dependencies

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 having the ‘Token Verification’ and optionally ‘Receipt Generation’ privileges control 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	Symmetric key or public asymmetric key to be used to verify a Token. To be protected from unauthorised modification and disclosure.
D.RECEIPT-GENERATION-KEY	Symmetric key or private asymmetric key to be used to generate Receipts. To be protected from unauthorised modification and disclosure.
D.CONFIRMATION-DATA	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	The attacker may generate fake receipts in order to hide or falsify completion proofs of card management operations.
T.TOKEN	The attacker may try to impersonate the Card Manager in order to gain access to the card and perform illegitimate card management operations.
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 that according to the methods defined in GlobalPlatform specifications. *Application Note*: See [GPCS] sections B.1, B.2, B.3, B.4, and C.5.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 that 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

Objectives	Threats, OSP
O.RECEIPT	T.RECEIPT
O.TOKEN	T.TOKEN
OE.TOKEN-GEN	OSP.TOKEN-GEN
OE.RECEIPT-VER	OSP.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:

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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) who requested 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

- **DES, AES, RSA, ECC**

and cryptographic key sizes

- **16-byte DES (its usage is no longer recommended)**
- **1024-bit RSA (its usage is no longer recommended)**
- **2048-bit RSA**
- **256-bit, 384-bit, or 512-bit ECC**
- **16-byte, 24-byte, or 32-byte AES**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

that meet the following: **[GPCS]**

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

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

- **DES, AES, RSA, ECC**

and cryptographic key sizes

- **16-byte DES (its usage is no longer recommended)**
- **1024-bit RSA (its usage is no longer recommended)**
- **2048-bit RSA**
- **256-bit, 384-bit, or 512-bit ECC**
- **16-byte, 24-byte, or 32-byte AES**

that meet the following: **[GPCS]**

Application Note:

The generation of 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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

11.5 Security Requirements Rationale

SFRs	Objectives
FCO_NRR.1/GP-RECEIPT	O.CARD-MANAGEMENT, O.RECEIPT
FCO_NRO.2/GP-TOKEN	O.CARD-MANAGEMENT, O.TOKEN
FCS_COP.1/GP-TOKEN	O.APPLI-AUTH, O.CIPHER, O.TOKEN
FCS_COP.1/GP-RECEIPT	O.APPLI-AUTH, O.RECEIPT, O.CIPHER

O.APPLI-AUTH This Security Objective is met by the following SFRs:

- FCS_COP.1/GP-TOKEN ensures that the card management command is authorised by verifying the Token signature.
- FCS_COP.1/GP-RECEIPT ensures that the card management command has been successfully processed by computing the Receipt signature.

11.6 SFR Dependencies

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])

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 that their Application code to be loaded onto the card have to be checked for integrity and authenticity. 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). It 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]. APSD cryptographic keys needed to verify Load File Data Block signatures. To be protected from unauthorised disclosure and modification.
Threats	
T.UNAUTHORISED-CARD-MNGT, 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

12.3.1 Security Objectives Rationale

Objectives	Threats, OSP
OE.DAP_BLOCK_GEN	OSP.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 **SHA-1, SHA-256, SHA-384, or SHA-512** and cryptographic key sizes **none** that meet the following: **NIST SP 800-57-1**.

Application Note:

See description in [GPCS] section C.3 for more details.

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 **DES, RSA, ECC, or AES** and cryptographic key sizes **16-byte DES, 1024-bit RSA, 2048-bit RSA, 256-bit, 384-bit, or 512-bit ECC, 16-byte, 24-byte, or 32-byte AES** that meet the following: **DES [ISO 9797-1], AES [NIST 800-38B], RSA [PKCS#1], ECC [ANSI X9.62]**.

Application Note:

Refer to the description in [GPCS] section C.3 for more details.

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

SFRs	Objectives
FCS_COP.1/GP-DAP_SHA	O.CARD-MANAGEMENT, O.LOAD, O.CIPHER, O.INSTALL, O.APPLI-AUTH
FCS_COP.1/GP-DAP_VER	O.CARD-MANAGEMENT, O.LOAD, O.CIPHER, O.INSTALL, O.APPLI-AUTH
FCO_NRO.2/GP-DAP	O.CARD-MANAGEMENT, O.LOAD, O.INSTALL, O.APPLI-AUTH

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

- 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.

12.6 SFR Dependencies

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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]. CASD cryptographic keys needed to verify 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’.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 with no 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)", using a mechanism that does not require the use of a Secure Channel to ensure the identity of the parties.
- 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 cryptographic keys generated on-card RGK with its 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.
Organisational Security Policies	
OSP.CCCM	APs who must not share the Secure Channel keys with the Issuer should use one of the CCCM Models.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

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

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: on-card random key generation]** 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 selected cryptographic operations from the table below]** in accordance with a specified cryptographic algorithm **[assignment: list of cryptographic algorithms from the table below]** and cryptographic key sizes **[assignment: list of cryptographic key sizes from the table below]** that meet the following: **[assignment: list of standards from the table below].**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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	16 bytes for TDES or 128 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	Keys longer than or equal to 1024 bits	[GPCS] section B.3
Pull Model (Asymmetric Key Mode)	Encryption of the RGK by the AP Public Key	RSA	Keys longer than or equal to 1024 bits	[GPCS] section B.3
Pull Model (Asymmetric Key Mode)	Signature of the RGS with the CASD Private Key	RSA	Keys longer than or equal to 1024 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	16 bytes for TDES or 128 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	16 bytes for TDES or 128 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	16 bytes for TDES or 128 bits for AES	[GPCS] section B.1 for TDES [GPCS] section B.2 for AES
Pull Model (Symmetric Key Mode)	Signature of the RGK with the CASD Signature Key	TDES or AES	16 bytes for TDES or 128 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	Keys longer than or equal to 1024 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	Keys longer than or equal to 1024 bits	[GPCS] section B.3
Push Model with or without AP certificate	Decryption of the APSD keys using the CASD private key	RSA	Keys longer than or equal to 1024 bits	[GPCS] section B.3

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Personalisation Models	Operation	Algorithm	Length	Recommended Standards
Push Model without AP certificate	Decryption of the APSD keys using the temporary APSD Secure Channel keys	RSA	Keys longer than or equal to 1024 bits	[GPCS] section B.3
Push Model without AP certificate	Signature verification of the APSD keys by the temporary APSD Secure Channel keys	RSA	Keys longer than or equal to 1024 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]

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 above table) 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 the table above should be selected.
- The ST writer should check the cryptographic operations implemented by the TOE against GlobalPlatform *Cryptographic Algorithm Recommendations* ([GP Crypto]).

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 to 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 to 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 h8shall 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.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- **[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]**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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] using a mechanism that does not require the use of a Secure Channel to ensure the identity of the parties.

14.5 Security Requirements Rationale

SFRs	Objectives	Rationale
FCS_CKM.1/GP-CCCM	O.KEY-MNGT, O.CIPHER, O.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, 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. 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]. FMT_MSA.1/GP-CCCM and FMT_MSA.3/GP-CCCM specify security attributes enabling to ensure the confidentiality of card management commands, and enforce the Confidential Personalisation of Secure Channel Keys.
FCS_COP.1/GP-CCCM	O.KEY-MNGT, O.CIPHER, O.CCCM	
FDP_IFC.2/GP-CCCM	O.DOMAIN-RIGHTS, O.COMM-AUTH, O.COMM-INTEGRITY, O.COMM-CONFIDENTIALITY, O.CCCM	
FDP_IFF.1/GP-CCCM		
FMT_MSA.1/GP-CCCM		
FMT_MSA.3/GP-CCCM		
FTP_ITC.1/GP-CCCM	O.COMM-CONFIDENTIALITY, O.CCCM	

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

14.6 SFR Dependencies

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 its base SE PP (core SE PP and packages).

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

15.1 TOE Type

The PP-Module for [Amd C] extends the TOE of the SE 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 GP Registry,
    - The CRS API; an extension of the GP 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 an Application interested in being 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: it 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	It contains the contactless Protocol Parameters. To be protected from unauthorised modification. *Application Note*: This asset is an extension of D.GP_REGISTRY.
Threats	
T.CL-REGISTRY-OVERWRITE	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).

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

T.COUNTERS-FREEZE	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.
T.CL-AUTH-FORGE	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.
T.CRS-BYPASS	The attacker grants the CRS privileges to unauthorised application in order to perform unauthorised state transitions (e.g. set a NON-ACTIVATABLE application to ACTIVATED or DEACTIVATED, or make it visible).

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. As the SET STATUS command is not protected, it mostly amounts to ensure that this command can only impact CRS-registered applications and cannot perform unauthorised state transitions. The Contactless Registry shall be protected for integrity 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 level “AUTHENTICATED” at least.
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

Objectives	Threats, OSP
O.CTL_REGISTRY	T.CTL-REGISTRY-OVERWRITE
O.CTL_SC	T.CTL-AUTH-FORGE
O.CRS_PRIVILEGES	T.CRS-BYPASS
O.CRS_COUNTERS	T.COUNTERS-FREEZE

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 States (ACTIVATED, DEACTIVATED, NON_ACTIVATABLE), Contactless privileges, Communication Interface Availability (Enabled, Disabled)**

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 CTL Application**
    - **There is at most one Application in the secure element that is assigned the Contactless Activation Privilege. This rule is enforced by the CRS/OPEN**
    - **An Application in the NON_ACTIVATABLE state is implicitly DEACTIVATED, and due to some internal reason known by the Application or its provider (e.g. a possible attempt of fraudulent use) cannot be ACTIVATED. Any attempt to activate an Application that is currently in the NON_ACTIVATABLE state, shall fail.**
    - **An Application cannot transition itself into the ACTIVATED state, except if it was granted the Contactless Self-Activation Privilege.**
    - **An Application cannot be activated if it is a Privacy-Sensitive Application and Non Privacy-Sensitive Applications are already activated, or conversely if it is a Non Privacy-Sensitive Application and Privacy-Sensitive Applications are already activated.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

  - **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.**

- **Other rules to be considered as referenced in the Application Note.**

- **[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: **none**.

FDP_ACF.1.4/GP-CTL The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **when at least one of the rules defined by [Amd C] does not hold.**

Application Note:

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- 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 has 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

SFRs	Objectives
FDP_ACC.1/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FDP_ACF.1/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FDP_ROL.1/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FMT_MSA.1/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FMT_MSA.3/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FMT_SMR.1/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FMT_SMF.1/GP-CTL	O.CTL_REGISTRY, O.CRS_COUNTERS, O.CRS_PRIVILEGES
FTP_ITC.1/GP-CTL	O.CTL_SC

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

15.6 SFR Dependencies

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
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 its base SE PP (core SE PP and packages).

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

16.1 Scope

This PP-Module extends the TOE of the SE 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 rather is 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 Executable Load File being upgraded. It is referred to as the “old ELF version”. To be protected from unauthorised modification.
D.NEW_ELF	The Executable Load File upgrading the old ELF version. It is referred to as the “new ELF version”. To be protected from unauthorised modification.
D.ELF_AID	Executable Load File AIDs defined in the old and new ELF versions. To be protected from unauthorised modification.
D.ELF_SESSION_ST	ELF Upgrade Session Status as described in [Amd H] Table 4-8. To be protected from unauthorised modification.
D.ELF_APP_INS	Application instances. To be protected from unauthorised modification and disclosure.
D.ELF_RG_DATA	Registry data includes any persistent on-card information relating to the Application instance that would not be stored/manipulated directly by the Application instance itself. To be protected from unauthorised modification.
Threats	
T.ELF-UNAUTHORISED	Attacker tries to load an unauthorised ELF.
T.ELF-VERSION	Attacker tries to change application version but prevent new ELF from being loaded.
T.ELF-DATA-ACCESS	Attacker tries to access confidential application instance data.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

T.ELF-DATA-INTEGRITY	Attacker tries to change application instance data.
T.ELF-SESSION	Attacker tries to perturb the Session Status to make incomplete upgrade seem complete.
T.ELF-ILL-COMMAND	Attacker tries to execute forbidden commands during the ELF upgrade session.
T.ELF-RES-DATA	Unauthorised access to data related to ELF through reallocation of TOE resources from one user or process to another.
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 at all occurs (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	ELF integrity shall be preserved during the loading process – (confidentiality maintained if required).
O.ELF_APP_DATA	Application instance data shall be securely stored when saved. The OPEN shall maintain the integrity & consistency of Registry data.
O.ELF_SESSION	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).
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

Threats, OSPs	Objective
T.ELF-UNAUTHORISED	O.ELF_AUTHORISED O.CARD-MANAGEMENT O.DOMAIN-RIGHTS O.COMM_AUTH
T.ELF-VERSION	O.ELF_INTEGRITY O.COMM_CONFIDENTIALITY O.COMM_INTEGRITY
T.ELF-DATA-ACCESS	O.ELF_APP_DATA
T.ELF-DATA-INTEGRITY	O.ELF_APP_DATA

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Threats, OSPs	Objective
T.ELF-SESSION	O.ELF_STATUS
T.ELF-ILL-COMMAND	O.ELF_STATUS
T.ELF-RES-DATA	O.ELF_DATA_PRO
OSP.ELF_DELE_OP	O.ELF_DELE_IRR

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 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.**
- **If multiple ELFs are upgraded within the same ELF Upgrade Session, each of the sequences of the Saving phase (Data saving, Cleanup, and Deletion) will be completed for all the ELFs before entering the next sequence.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- **During the Deletion Sequence of the Saving Phase, the S.OPEN attempts to delete the ELF(s) and all its (their) Application instances.**
- **Card Content Management Operations described in [Amd H] will always be rejected during an ELF Upgrade Session.**
- **S.OPEN allows an ELF upgrade session to be initiated if no other ELF upgrade session is running.**
- **S.OPEN saves the data of the Application being updated associated by AID.**
- **S.OPEN deletes the application instance once the app data has been saved associated by AID.**
- **S.OPEN deletes the ELF original when all application instance data sets have been saved.**
- **S.OPEN confirms that the ELF Upgrade has been successfully loaded.**
- **S.OPEN restores the saved application if the ELF Upgrade has been successful.**
- **[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: **none**.

FDP_ACF.1.4/GP-ELFU The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **when at least one of the rules defined by [Amd H] does not hold.**

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) has already started, then it shall automatically restart and complete upon next power up.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

- **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 or the ELF Upgrade Recovery Procedure, 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]**.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

16.5 Security Requirements Rationale

Objective	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 an entity authenticated against the security domain which the ELF belongs to 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 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 assured by using 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 by ensuring that corrupted application data cannot be used
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 authenticating the origin of the APDU commands that the card receives.
O.ELF_DELE_IRR	FDP_ROL.1/GP-ELFU	FDP_ROL.1/GP-ELFU contributes to this Objective by ensuring that the deletion operation is completed properly.
O.ELF_DATA_PRO	FDP_RIP.1/ADEL	FDP_RIP.1/ADEL is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

16.6 SFR Dependencies

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 base SE PP (core SE PP and packages).

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

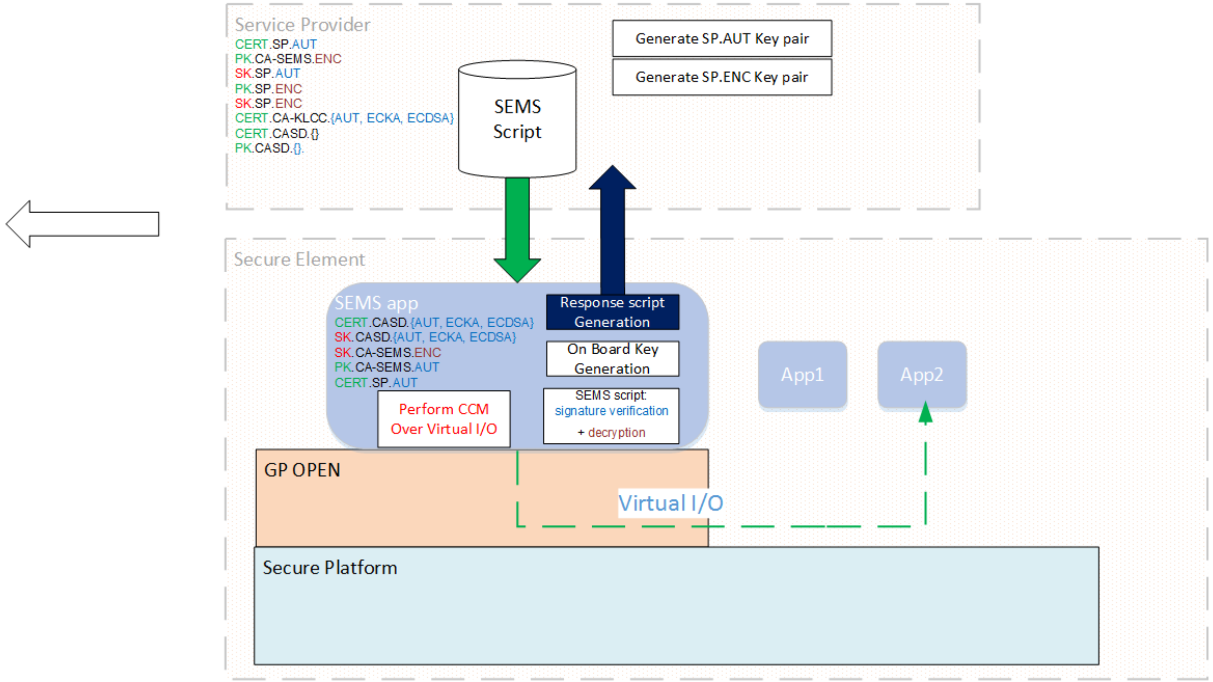
17.1 Overview

Amendment I ([Amd I]), Secure Element Management Service, provides a means to reduce the Card Content Management costs. 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 up to a certain number of times on those particular SEs through SEMS.

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

17.1.4 SEMS Roles

The main roles participating in the SEMS mechanism are:

- The SEMS Certification Authority (CA-SEMS)
- The Key Loading Card Certificates Certification Authority (CA-KLCC)
- The Service Provider (SP)
- The SEMS Application Provider – Requires strong trust relationship with CA-SEMS

These roles are more fully described in [Amd I].

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

17.1.5 SEMS Cryptographic Keys

SEMS cryptography relies upon five pairs of asymmetric keys. Each keypair has a private key, prefixed by SK, and an associated public key, prefixed by PK; e.g. SP.AUT has keypair {SK.SP.AUT, PK. SP.AUT}.

Key Name	Description
CA-SEMS.ENC	These keys are used to decrypt / encrypt SEMS scripts. The key pair is owned by the SEMS Certification Authority (CA-SEMS). The immediate purpose of this key pair is to protect the key used for encryption and decryption of the SEMS script. • The private key SK.CA-SEMS.ENC is stored within the SEMS Application. • The public key PK.CA-SEMS.ENC is provided to the Service Provider by the CA-SEMS.
CA-SEMS.AUT	These keys are used to generate / verify a certificate signature. The key pair is owned by CA-SEMS. • The private key SK.CA-SEMS.AUT is kept in the CA-SEMS environment. It is used to sign the CERT.SP.AUT certificates that are provided to SPs that are given the right to perform certain CCM operations with the SEMS scripts. • The public key PK.CA-SEMS.AUT is stored within the SEMS Application. It is used to verify the signature of the CERT.SP.AUT certificate contained in the SEMS script. After the personalisation of the SEMS Application, the PK.CA-SEMS.AUT key may be rotated.
SP.AUT	These keys are used to generate / verify the SEMS script signature. The key pair is owned by the Service Provider. A Service Provider may own several CERT.SP.AUT certificates. • The private key SK.SP.AUT is stored in the secure environment of the Service Provider. It is used to sign a SEMS script. • The public key PK.SP.AUT is stored within the CERT.SP.AUT certificate which is signed with the CA-SEMS private key SK.CA-SEMS.AUT. This key is used to verify the signature of a SEMS script.
CASD. **{AUT,ECKA,ECDSA}**	These keys are used to sign / verify the authenticity and the integrity of the on-board generated key or for an EC Key Agreement (ECKA). The key pair for CASD.ECDSA might (in this version of this specification) be stored in the SEMS Application whereas the other two key pairs (regarding CASD.AUT and CASD.ECKA) are supposed to be stored in the CASD with KVN '74' (according to [Amd A]). The location of the corresponding private keys and their associated certificates (containing the respective public key) are implementation specific. • The private keys SK.CASD.{AUT, ECKA, ECDSA} are stored in the SE and used to sign the on-board generated keys (OBGK) returned by the SEMS Application or used in ECKA. • The public keys PK.CASD.{AUT, ECKA, ECDSA} are stored in the CERT.CASD.{AUT, ECKA, ECDSA} certificates which are signed by the respective SK.CA-KLCC.{AUT, ECKA, ECDSA} (root) private key of the CA-KLCC. • The (SK.CASD.ECDSA, PK.CASD.ECDSA) key pair is mandatory while (SK.CASD.AUT, PK.CASD.AUT) and (SK.CASD.ECKA, PK.CASD.ECKA) are optional.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Key Name	Description
SK.SP.ENC.{S1,S4}, PK.SP.ENC.{S1,S4} or SK.SP.ECKA.S3, PK.SP.ECKA.S3	Depending on the scenario, these keys are used to encrypt / decrypt the SD key generated by the SEMS Application or for a key agreement, the SP generates these keys once. • The private key SK.SP.ENC.{S1,S4} or SP.PK.ECKA.S3 is stored in the Service Provider secure environment. • The public key PK.SP.ENC.{S1,S4} or PK.SP.ECKA.S3 is inserted within SEMS scripts in the SEMS command triggering the on-board key generation. The SEMS Application applies the encryption of the on-board generated key with PK.SP.ENC on behalf of the SP or uses an ECKA algorithm.

17.1.6 Cryptographic Algorithm Details

17.1.6.1 ECC Curve

The current version of this specification supports only curves with ECC key lengths of 256 bits according to [GPCS] Table B-1. CERT.SP.AUT tag '7F49' sub-tag '8F' may explicitly identify the ECC curve according to [GPCS] Table B-2. If CERT.SP.AUT does not include this optional parameter information, the ECC public key PK.SP.AUT (contained in sub-tag '86' of tag '7F49' shall be based on the ECC curve brainpoolP256r as specified in the Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation ([RFC 5639]).

17.1.6.2 ECDH

The Elliptic Curve Diffie-Hellman shall be performed according to [NIST 800-56A].

17.1.6.3 ECDSA

The ECDSA shall be performed as specified in [GPCS] section B.4.3.

17.1.6.4 AES-CBC

The AES in CBC mode for encryption and decryption shall be performed as specified in the NIST Special Publication 800-38A ([NIST 800-38A]) with Initial Vector equal to 0 and no padding.

17.1.6.5 Key Derivation Function (KDF)

The KDF returns the most significant 128 bits of the applied Hashing algorithm SHA-256 as defined in [NIST 800-56A]. These returned most significant 128 bits become the AES key K.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

17.2 Security Problem Definition

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

Table 17-1: SPDs of SEMS PP-Module

Assets (in transit)	
D.SEMS-APPLICATION-CODE	To be protected from unauthorised modification and disclosure.
D.SEMS-APPLICATION-DATA	To be protected from unauthorised modification and disclosure.
D.SEMS-PERSONALISATION-DATA	To be protected from unauthorised modification and disclosure.
D.SEMS-KEYS	To be protected from unauthorised modification and disclosure.
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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.

The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Threats	
T.SEMS-IMPERSONATE	An Attacker tries to impersonate a SEMS script or corrupt the content of a SEMS script. *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.
OSP	
OSP.SEMS_OPEN_ACCESS	Access to this virtual I/O is reserved for the SEMS application.
OSP.SEMS_OPEN_ROUTING	The OPEN will verify that the CERT.SP.AUTH embedded in the SEMS script matches that which is loaded on the target application, with tag '5F20', before routing the C-APDUs to the application.
Assumptions	
A.VIRTUAL_IO_TRUST	There exists a trust relationship between the Security Domain, receiving the Command APDUs via the Virtual I/O, and the SEMS Application, based on the CERT.SP.AUT certificate holder identifier saved in the registry during the install operation and checked by the OPEN during APDU forwarding on the virtual I/O Interface.

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 Security 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	The TOE shall address the confidential card content management requirements defined in [Amd I] section 2.
O.SEMS_SCRIPT_AUTH	Verify script Authenticity and origin by verifying the CERT.SP.AUT and signature.
O.SEMS_COMMAND_AUTH	Decrypt and verify integrity of SEMS commands embedded in the SEMS script.
O.SEMS_ENFORCE	The TOE shall enforce the rules defined in [Amd I] section 4.11.
Security Objectives for the Operational Environment	
OE.SEMS_OPEN	The OPEN will provide a virtual I/O interface for exclusive use of the S.AP_SEMS 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

OE.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.
OE.APP_PROVIDER	The SEMS App provider maintains a secure environment where SK.SP.AUT is stored and 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 SEMS scripts to be routed from SEMS application to target application.

The list of SFRs proposed are:

Proposed SFR	Analysis
FCS_CKM.1/DH_SEMS	Cryptographic key generation – Diffie-Hellman for SEMS
FCS_CKM.4	Cryptographic key destruction – Session keys
FCS_COP.1/SEMS_ENC	Cryptographic Operation – Encryption / Decryption
FCS_COP.1/SEMS_MAC	Cryptographic Operation – Message Authentication Code
FCS_COP.1/SEMS_SIG_VER	Cryptographic Operation – Digital Signature Verification
FCS_RNG.1	Cryptographic Operation – Generation of Random Numbers
FMT_SMR.1/SEMS	Specification of Management Functions: • CA-SEMS (SEMS Certification Authority) • AP-SEMS (SEMS Application Provider) • Service Provider (holder of SEMS SP certificate)
FCO_NRO.2/SEMS	Enforced Proof of Origin

FCO_NRO.2/GP-SEMS Enforced proof of origin

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

FCO_NRO.2.2/GP-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/GP-SEMS The TSF shall provide a capability to verify the evidence of origin of information to **originator** given **at the time the SEMS script is processed.**

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

FDP_ACC.1/GP-SEMS Subset access control

FDP_ACC.1.1/GP-SEMS The TSF shall enforce the **SEMS Management policy** on **SEMS Scripts.**

FMT_SMF.1/GP-SEMS Specification of management functions

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

- **Transmit Card Content Management C-APDUs over a Virtual I/O channel**

FMT_SMR.1/GP-CTL Security roles

FMT_SMR.1.1/GP-SEMS The TSF shall maintain the roles **S.CA-SEMS, S.CA-KLCC, S.SP_SEMS, S.AP_SEMS**.

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

FIA_UID.1/SEMS Timing of identification

FIA_UID.1.1/GP-SEMS 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-SEMS The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

17.5 SFR Dependencies

SFR	Dependencies
FCS_CKM.1	(FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction
FCS_CKM.4	(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_COP.1	(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
FCO_NRO.2/SEMS	FIA_UID.1 Timing of identification
FCS_RNG.1	No dependencies
FDP_ACC.1	FDP_ACF.1
FMT_SMF.1	No dependencies
FMT_SMR.1	FIA_UID.1 Timing of identification
FIA_UID.1	No dependencies

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 OS update is addressed here, not 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 Card Framework. Some additional plugins might be present in the OS as well 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 already been introduced in the core SE PP.
- For this separation of roles to be enforced, dedicated cryptographic keys shall be owned and used by the OS Developer to support the OS Update capability, in order to ensure the confidentiality of the additional code transmitted to the TOE and 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

18.2 SPD

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

Assets	
D.OS-UPDATE_SGNVER-KEY	Refinement of D.APP_KEYS. It is 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. Case of a symmetric key: to be protected from unauthorised disclosure and modification. Case of an asymmetric public key: to be protected from unauthorised modification.
D.OS-UPDATE_DEC-KEY	Refinement of D.APP_KEYS. It is 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	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	Identification data associated to 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 be also protected from unauthorised disclosure (confidentiality requirement) to not permitting an attacker to determine if 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

Threats	
T.UNAUTHORISED-TOE-CODE-UPDATE	An attacker loads malicious additional code in order to compromise the security features of the TOE. Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.
T.FAKE-SGNVER-KEY	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. Targeted assets: D.OS-UPDATE_SGNVER-KEY, D.OS-UPDATE_ADDITIONALCODE.
T.WRONG-UPDATE-STATE	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. Targeted asset: D.OS-UPDATE-CODE-ID.
T.INTEG-OS-UPDATE-LOAD	The attacker modifies (part of) the additional code when it is transmitted to the TOE for installation. Targeted assets: D.OS-UPDATE_ADDITIONALCODE, D.JCS_CODE, D.JCS_DATA.
T.CONFID-OS-UPDATE-LOAD	The attacker discloses (part of) the additional code when it is transmitted to the TOE for installation. Targeted assets: 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

OSP.ADDITIONAL_CODE_SIGNING	The additional code has to be signed with a cryptographic key according to relevant standard and the generated signature is associated to the additional code. The additional code signature must be checked 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 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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). 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 (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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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

Objectives	Threats, OSP
O.SECURE_LOAD_ACODE	OSP.ADDITIONAL_CODE_SIGNING, T.UNAUTHORISED-TOE-CODE-UPDATE, T.FAKE-SGNVER-KEY
O.SECURE_AC_ACTIVATION	OSP.ATOMIC_ACTIVATION, T.WRONG-UPDATE-STATE
O.TOE_IDENTIFICATION	OSP.TOE_IDENTIFICATION, T.WRONG-UPDATE-STATE
O.CONFID-OS-UPDATE.LOAD	OSP.ADDITIONAL_CODE_ENCRYPTION, T.CONFID-OS-UPDATE-LOAD
OE.OS-UPDATE-EVIDENCE	A.OS-UPDATE-EVIDENCE
OE.OS-UPDATE-ENCRYPTION	OSP.ADDITIONAL_CODE_ENCRYPTION
OE.SECURE_ACODE_MANAGEMENT	A.SECURE_ACODE_MANAGEMENT

18.4 Security Functional Requirements

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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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.

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, who responsible for verifying the signature and decrypting the additional code before authorising its loading, installation, and activation, [assignment: list of other subjects covered by the SFP]**
- **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]**.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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, therefore preventing any additional code from being installed until the additional code signature is actually successfully verified by the TOE.

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.

In case that 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

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 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 by cancelling the operation (the TOE remains the Initial TOE) or entering an error state, and consistency is maintained 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

SFRs	Objectives
FDP_ACC.1/OS-UPDATE	O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION, O.CONFID-OS-UPDATE.LOAD
FDP_ACF.1/OS-UPDATE	O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION, O.CONFID-OS-UPDATE.LOAD
FIA_ATD.1/OS-UPDATE	O.TOE_IDENTIFICATION
FMT_MSA.3/OS-UPDATE	O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION, O.CONFID-OS-UPDATE.LOAD
FMT_SMR.1/OS-UPDATE	O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION, O.CONFID-OS-UPDATE.LOAD
FMT_SMF.1/OS-UPDATE	O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION, O.TOE_IDENTIFICATION, O.CONFID-OS-UPDATE.LOAD
FTP_TRP.1/OS-UPDATE	O.CONFID-OS-UPDATE.LOAD
FCS_COP.1/OS-UPDATE-DEC	O.CONFID-OS-UPDATE.LOAD

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

SFRs	Objectives
FCS_COP.1/OS-UPDATE-VER	O.SECURE_LOAD_ACODE

18.6 SFR Dependencies

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 GP 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.

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

18.7 Consistency Rationale

The OS Update PP-Module is consistent with its base SE PP (core SE PP and packages).

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

Copyright © 2017-2020 GlobalPlatform, Inc. All Rights Reserved.
The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.