Giesecke+Devrient

Security Target Lite Sm@rtSIM Polaris SGP.22/SGP.32

Giesecke+Devrient Mobile Security

Public

Table of Contents

1. ST Introduction

1.1 Security Target Reference

Name	Security Target Lite Sm@rtSIM Polaris SGP.22/SGP.32
Version	Version 1.6 / 12 March 2025
Reference	GDM_Sm@rtSIM_Polaris_SGP.22 and SGP.32_ASE_Lite
ST template reference	[SGP.17]

1.2 TOE reference

Name	Sm@rtSIM Polaris SGP.22/SGP.32
Version	1.0
Reference	Sm@rtSIM Polaris SGP.22/SGP.32

1.3 TOE scope

1.3.1 Physical scope

Category	**Component**	**Version**	**Delivery form**
HW	ST33K1M5C CC certificate: NSCIB-CC-2300056-02-CERT [IC_ST]	IC Version D	wafer and package
	ST33K1M5A and ST33K1M5M B03	IC Version B	wafer and package

	CC certificate: NSCIB-CC-2300112-02 [IC 2_ST]		
FW	ST33K platform firmware	FW Version 3.1.4	Binary in memory
SW	Sm@rtSIM NextGeneration Polaris	2.0	Binary in memory
DOC	Operative guidance	[AGD_OPE]	pdf file
DOC	Preparative guidance	[AGD_PRE]	pdf file
DOC	Security guidance	[AGD_SEC]	pdf file

1.3.2 Logical scope

The logical scope of the TOE is the scope of the ST TOE as defined in [PP-eUICC] and section 1.4 and subsections in this ST.

1.4 TOE Overview

The TOE is the embedded UICC software that implements:

- The GSMA Remote SIM Provisioning (RSP) Architecture for Consumer Devices ([SGP.21] and [SGP.22]).
- GSMA eSIM IoT Architecture and Requirements [SGP.31] and eSIM IoT Technical Specification [SGP.32] for IoT Devices

As Runtime Environment, the TOE uses Java Card version 3.1. A detailed TOE overview is given in chapter 1.2 of [PP-eUICC]. To enable to update an already installed embedded OS, the TOE contains the Image Trusted Loader (ITL) software.

This Security Target is following scenario 3 of the Protection Profile Usage, according to [PP-eUICC], chapter 1.2.5. It is written to accomplish a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

1.4.1 TOE Description

The TOE is a “whole eUICC” as defined in chapter 1.2.1 of [PP-eUICC] including:

- The complete TOE of the Base-PP (the Application Layer and the Platform layer as shown in Figure 1);
- The secure IC platform and OS;
- The Runtime Environment (the Java Card System);
- The GlobalPlatform Card Content Management;
- The Image Trusted Loader (ITL), which is a module that enables a full Operating System update. This update can be performed both in the factory (Over The Wire) or in the field (Over The Air), when the previous OS is already installed.

1.4.2 TOE type and usage

The TOE type is a composite of secure software implemented on secure IC. The eUICC is an UICC embedded in a consumer device or IoT device. The TOE scope is shown in Figure 1.

The secure software is configured to operate either as a consumer or IoT device during the pre-personalization (phase c of the TOE life-cycle). Therefore, the TOE cannot support both configurations at the same time after the TOE-delivery.

During the operational usage (Phase e), the configuration of the secure software shall be identified using the *iotSpecificInfo* field, which is included in the response data for *EuiccInfo2*, as defined in section 5.9.2 of [SGP.32].

The expected value of is:

iotSpecificInfo	Response (SGP.32 v1.2.0)
- **IoT Version** - eCallSupported - fallbackSup-ported	B4 0B A0 05 **04 03 <u>01 02 00</u>** 81 00 82 00

The iotSpecificInfo field is not included in the response data for EuiccInfo2 defined in section 5.7.8 of [SGP.22]. Therefore, when the TOE is configur-ated as consumer device, this field is empty.

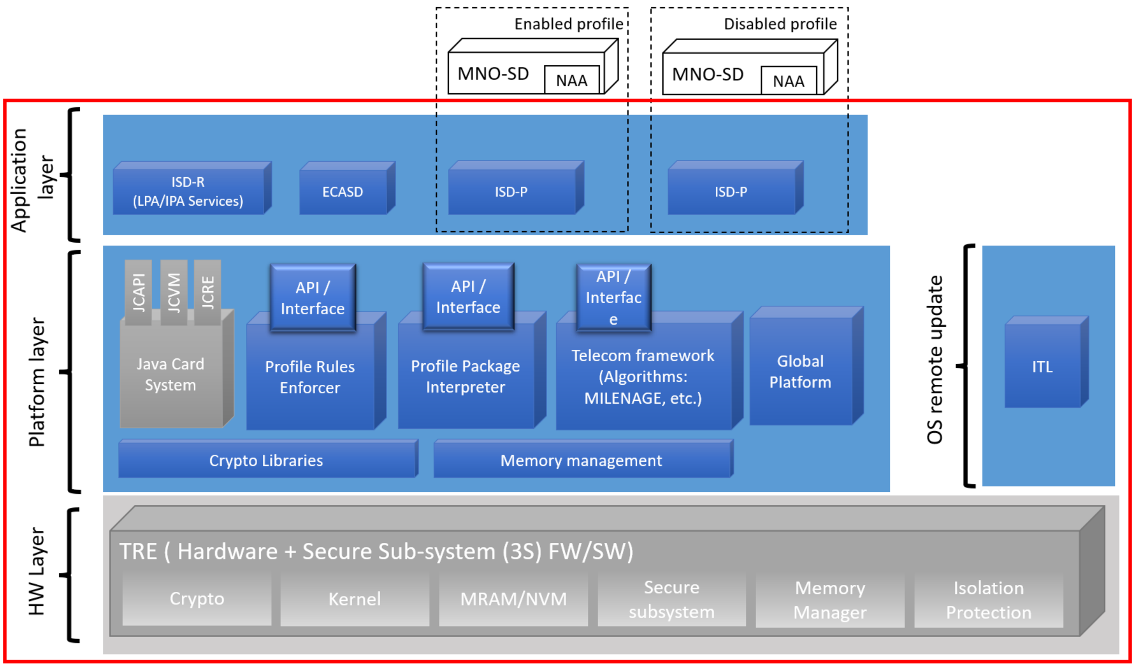

Figure 1 TOE Scope

1.4.3 TOE life cycle

The lifecycle of the TOE is as described in [PP-eUICC], Section 1.2.3.

The delivery of the self-protected TOE happens at the end eUICC lifecycle Phase d as shown in Table 1.

eUICC life Phase e: operational usage of the TOE includes the activities related OS updates, in addition to those listed in [PP-eUICC], Section 1.2.3.1.

TOE	PP-0084 lifecycle	eUICC lifecycle
TOE Development	Phase 1 Security IC Embedded Software Development	Phase a eUICC Platform Development Development of IC and Embedded Software
	Phase 2 Security IC Development	
TOE storage, pre-perso, test	Phase 3 Security IC Manufacturing	Phase b eUICC platform storage, pre-perso, test Security IC manufacturing and packaging
	Phase 4 Security IC Packaging	
	Phase 5 Composite Product Integration	Phase c eUICC platform storage, pre-perso, test Integration of Platform Software and Applications
TOE personalisation	Phase 6 Personalisation	Phase d eUICC Personalisation Addition of applications (profiles, ISD-P)

TOE delivery

Table 1 TOE life-cycle phases and TOE delivery

1.4.4 Non-TOE HW/SW/FW available to the TOE

Non-TOE is same than the ones mentioned in the [PP-eUICC], section 1.2.4, except for Integrated Circuit (IC) or Chip, Embedded software (ES) and the Runtime Environment, which are part of the TOE.

Basic applications must be compliant with the security rules as defined in [GP SG]. Bytecode verifier must be used, which is considered as not part of the TOE.

The Profiles are not part of the TOE.

Figure 2 shows the TOE interfaces covered by the ST:

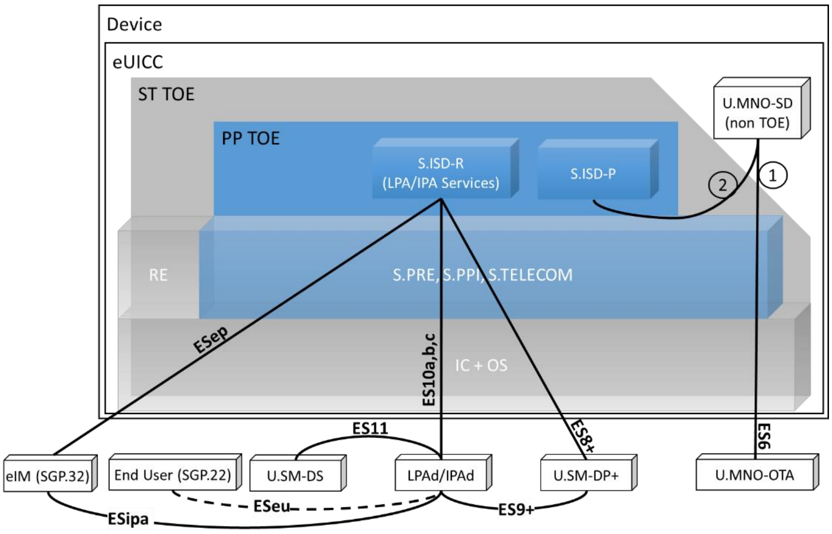

Figure 2 TOE interfaces IPAd/LPAd

2. Conformance Claims

2.1 CC conformance claims

This ST claims conformance to Common Criteria 2022: CC Part 1 [CC1], CC Part 2 [CC2] (extended), CC Part 3 [CC3] (conformant).

2.2 CC Part 5 [CC5]

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

ADV_ARC is refined to add a particular set of verifications on top of the existing requirement.

2.3 PP claim

This ST claims *demonstrable* conformance to the Protection Profile [PP-eUICC].

2.4 Package claim

The assurance requirement of this Security Target is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

ADV_ARC defined in [PP-eUICC] is refined to add a particular set of verifications on top of the existing requirement.

2.5 Conformance Claim Rationale

This Security Target is conformant to the claimed PP.

The TOE of this Security Target is the whole embedded UICC made of the IC, OS, RE, the TOE of the Base-PP (described in sections 1 to 6 in [PP-eUICC]) and the PP Module OS Update (Annex A).

The objectives for the environment (that is for the IC, OS and RE) specified in the Protection Profile have become objectives for the TOE in this Security

Target. These objectives have been partly fulfilled by a previous certificate (of an already certified IC) and partly translated in to SFRs.

The Security Problem Definition in this ST is taken directly from the [PP-eUICC] (chapter 3) with the changes described therein.

The Security Requirements in this ST have been taken directly from the [PP-eUICC] (chapter 6) and operations as appropriate have been performed.

The following notation used in the consistency tables in section 2.5.3:

(E) Equivalent: The element in the ST is the same as in [PP-eUICC].

(R) Refinement: The element in the ST refines the corresponding [PP-eUICC] element. New names are given between brackets and added to the list of elements.

(A) Addition: The element is newly defined in the ST; it is not present in [PP-eUICC] and does not affect it. Additions are either from [PP-JCS], [PP-GP] or TOE proprietary.

X: The element is present in [PP-eUICC].

2.5.1 Conformity of the TOE Type

The TOE type for this ST is the same as defined in the [PP-eUICC].

The TOE follows the third scenario from the definition in [PP-eUICC] (chapter 1.2.5) when the embedded eUICC is embedded in a certified IC, but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs in order to meet the objectives for the OS and JCS. This is a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

2.5.2 This STs additions and refinements to the PP

The security objectives for the environment concerning the smart card platform (IC) and the runtime environment (RE) have been changed into objectives for the TOE.

To cover the IC objectives, the following SFR is introduced: FPT_PHP.3.

Since the Runtime Environment is part of the TOE of this ST, SFRs defined in [PP-JCS] are included in this ST as indicated in 2.5.3.9, Table 10.

The SFRs from [PP-GP] are added to fulfill the secure card content management activities.

This ST defines SFRs for the post-delivery loading of code ("in-the-field-loading", abbreviated ITL) and secure personalization process.

2.5.3 SPD Consistency

2.5.3.1 Introduction

Most of the SPDs apply to both configurations of the TOE. However, some of the SPDs are unique to either [SGP.22] or [SGP.32] configuration.

In cases where an SPD is unique to one configuration, this is indicated by referencing the applicable specification in brackets: (SGP.22) or (SGP.32).

When no specification is referenced, the SPD applies to both configurations.

For example, in section 2.5.3.3 for users:

- U.MNO-SD: it applies to both configurations.
- U.eIM (SGP.32): it is specific to [SGP.32] configuration.
- U.End-User (SGP.22): it is specific to [SGP.22] configuration.

2.5.3.2 Assets consistency

The table below indicates the assets' consistency and the additions from [PP-JCS].

Assets	**PP-eUICC**	**Security Target**
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_ RULES	X	(E)

D.PRO-FILE_USER_CODES (SGP.22)	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)
D.PK.EIM.ECDSA (SGP.32)	X	(E)
D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(E)
D.APP_C_DATA		(A) Added from [PP-JCS].
D.APP_I_DATA		(A) Added from [PP-JCS].
D.API_DATA		(A) Added from [PP-JCS].
D.JCS_DATA		(A) Added from [PP-JCS].
D.SEC_DATA		(A) Added from [PP-JCS].
D.APP_KEYs		(A) Added from [PP-JCS].

D.PIN		(A) Added from [PP-JCS].
D.APP_CODE		(A) Added from [PP-JCS].
D.JCS_CODE		(A) Added from [PP-JCS].
D.CRYPTO		(A) Added from [PP-JCS].
D.UPDATE_IMAGE	X	(E): from OS Update module
D.TOE_IDENTIFIER	X	(E): from OS Update module
D.OS-UPDATE_KEY(S)	X	(E): from OS Update module

Table 2 Assets Consistency

2.5.3.3 Users and Subjects consistency

All Users defined in [PP-eUICC], section 3.2.1 (Base-PP), are relevant for the TOE of this Security Target. The table below indicates the Users' consistency.

User	**PP-eUICC**	**Security Target**
U.SM-DP+	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.eIM (SGP.32)	X	(E)
U.End-User (SGP.22)	X	(E)

Table 3 Users consistency

All Subjects defined in [PP-eUICC], section 3.2.2, and in the PP module OS Update, A.2.4, are relevant for the TOE of this Security Target. The table below indicates the Subjects' consistency and the additions from [PP-JCS] and [PP-GP].

Subjects	PP-eUICC	Security Target
S.ISD-R	X	(E)
S.ISD-P	X	(E)
S.ECASD	X	(E)
S.PPI	X	(E)
S.PRE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A) Added from [PP-JCS].
S.APPLET		(A) Added from [PP-JCS].
S.BCV		(A) Added from [PP-JCS].
S.CAD		(A) Added from [PP-JCS].
S.INSTALLER		(A) Added from [PP-JCS].
S.JCRE		(A) Added from [PP-JCS].
S.JCVM		(A) Added from [PP-JCS].
S.LOCAL		(A) Added from [PP-JCS].
S.MEMBER		(A) Added from [PP-JCS].
S.CAP_FILE		(A) Added from [PP-JCS].
S.SD		(A) Added from [PP GP].
S.OPEN		(A) Added from [PP GP].
S.OSU	X	(E): from OS Update module
S.UpdateImageCreator	X	(E): from OS Update module

Table 4 Subjects Consistency

2.5.3.4 Threats consistency

All Threats defined in [PP-eUICC], section 4.3.1, and in the PP module OS update, A.2.3, are relevant for the TOE of this Security Target. The table below indicates the Threats' consistency and the refinements from [PP-JCS].

Threats	**PP-eUICC**	**Security Target**
T.UNAUTHORIZED-PROFILE-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-PLATFORM-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-ELIGIBILITY	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-IDENTITY-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.IDENTITY-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-eUICC	X	(E)
T.LPAd-INTERFACE-EXPLOIT	X	(E)
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)

T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threat-ened assets.
T.PHYSICAL-ATTACK	X	(E)
T.CONFID-UPDATE-IM-AGE.LOAD	X	(E): from OS Update module
T.UNAUTH-UPDATE-IM-AGE.LOAD	X	(E): from OS Update module
T.INTEG-UPDATE-IM-AGE.LOAD	X	(E): from OS Update module
T.INTERRUPT_OSU	X	(E): from OS Update module

Table 5 Threats Consistency

2.5.3.5 Organizational Security Policies consistency

All Organizational Security Policies defined in [PP-eUICC], section 3.4, are relevant for the TOE of this Security Target. The table below indicates the Organizational Security Policies' consistency.

OSPs	**PP-eUICC**	**Security Target**
OSP.LIFE-CYCLE	X	(E)

Table 6 Organizational Security Policies Consistency

2.5.3.6 Assumptions consistency

All Assumptions defined in [PP-eUICC], section 3.5, are relevant for the TOE of this Security Target. A.CAP_FILE is defined as in [PP-JCS].

Assumptions	**PP-eUICC**	**Security Target**
A.TRUSTED-PATHS-LPAd-IPAd	X	(E)

A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.CAP_FILE		(A): Added from [PP-JCS]

Table 7 Assumptions Consistency

2.5.3.7 Objective for the TOE consistency

All Security Objectives defined in [PP-eUICC], section 4.1, and in the PP Module OS Update, A.3.1, are relevant for the TOE of this Security Target.

Note that OE.RE* and OE.IC* from [PP-eUICC] become security objectives for the TOE in the present Security Target. The [PP-eUICC] already provides the conversion of OE.RE* to objectives from the [PP-JCS] protection profile.

O.TOE	PP-eUICC	Security Target
O.PPE-PPI	X	(E)
O.eUICC-DOMAIN-RIGHTS	X	(E)
O.SECURE-CHANNELS	X	(E)
O.INTERNAL-SECURE-CHANNELS	X	(E)
O.PROOF_OF_IDENTITY	X	(E)
O.OPERATE	X	(E)
O.API	X	(E)
O.DATA-CONFIDENTIALITY	X	(E)
O.DATA-INTEGRITY	X	(E)
O.ALGORITHMS	X	(E)
O.IC.PROOF_OF_IDENTITY		Replaces OE.IC.PROOF_OF_IDENTITY defined in PP-eUICC
O.IC.SUPPORT		Replaces OE.IC.SUPPORT defined in PP-eUICC
O.IC.RECOVERY		Replaces OE.IC.RECOVERY defined in PP-eUICC
O.RE.PRE-PPI		Replaces OE.RE.PRE-PPI defined in PP-eUICC
O.RE.SECURE-COMM		Replaces OE.RE.SECURE-COMM defined in PP-eUICC

O.RE.API		Replaces OE.RE.API defined in PP-eUICC
O.RE.DATA-CONFIDENTIAL-ITY		Replaces OE.RE.DATA-CON-FIDENTIALITY defined in PP-eUICC
O.RE.DATA-INTEGRITY		Replaces OE.RE.DATA-INTEG-RITY defined in PP-eUICC
O.RE.IDENTITY		Replaces OE.RE.IDENTITY de-fined in PP-eUICC
O.RE.CODE-EXE		Replaces OE.RE.CODE-EXE defined in PP-eUICC
O.SECURE_LOAD_ACODE	X	(E): from OS Update module
O.CONFID-UPDATE-IM-AGE.LOAD	X	(E): from OS Update module
O.TOE_IDENTIFICATION	X	(E): from OS Update module
O.AUTH-LOAD-UPDATE-IM-AGE	X	(E): from OS Update module
O.SECURE_AC_ACTIVATION	X	(E): from OS Update module

Table 8 Security objectives for the TOE consistency

2.5.3.8 Objective for Environment consistency

O.ENV	**PP-eUICC**	**Security Target**
OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.MNO	X	(E)
OE.TRUSTED-PATHS-LPAd-IPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.MNO-SD	X	(E)
OE.EIM (SGP.32)	X	(E)
OE.CODE-EVIDENCE		(A): Added from [PP-JCS].
OE.CAP-FILE		(A): Added from [PP-JCS].
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF_IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PRE-PPI	X	Removed and replaced by O.RE.PRE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.

OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTI-ALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY.
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY.
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE.
OE.CONFID_UPDATE_IM-AGE.CREATE	X	(E): from OS Update module.

Table 9 Security Objectives for the Operational Environment Consistency

2.5.3.9 SFR consistency

All SFRs in [PP-eUICC] are relevant for the TOE of this Security Target.

SFR	PP-eUICC	Security Target
FIA_UID.1/EXT	X	Assignment performed.
FIA_UAU.1/EXT	X	Assignment performed.
FIA_USB.1/EXT	X	Selection performed.
FIA_UAU.4/EXT	X	Selection performed.
FIA_UID.1/MNO-SD	X	Assignment performed.
FIA_USB.1/MNO-SD	X	(E)
FIA_ATD.1/Base	X	Selection performed.
FIA_API.1	X	(E)
FDP_IFC.1/SCP	X	(E)
FDP_IFF.1/SCP	X	Assignment performed.
FTP_ITC.1/SCP	X	Assignment performed.
FDP_ITC.2/SCP	X	Assignment performed.
FPT_TDC.1/SCP	X	Assignment performed.
FDP_UCT.1/SCP	X	(E)
FDP_UIT.1/SCP	X	(E)
FCS_CKM.1/SCP-SM	X	Assignment performed.
FCS_CKM.2/SCP-MNO	X	Selection and Assignment performed.

SFR	PP-eUICC	Security Target
FCS_CKM.6/SCP-SM	X	Selection and Assignment performed.
FCS_CKM.6/SCP-MNO	X	Selection and Assignment performed.
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	Selection and Assignment performed.
FDP_ACC.1/ECASD	X	Assignment performed.
FDP_ACF.1/ECASD	X	Assignment performed.
FDP_IFC.1/Platform_services	X	Selection performed.
FDP_IFF.1/Platform_services	X	Selection and Assignment performed.
FPT_FLS.1/Platform_services	X	Selection and Assignment performed.
FCS_RNG.1	X	Selection and assignment performed.
FPT_EMS.1/Base	X	Assignment performed.
FDP_SDI.1/Base	X	(E)
FDP_RIP.1/Base	X	(E)
FPT_FLS.1/Base	X	(E)
FMT_MSA.1/PLATFORM_DATA	X	(E)

SFR	PP-eUICC	Security Target
FMT_MSA.1/RULES	X	Selection performed.
FMT_MSA.1/CERT_KEYS	X	Selection performed.
FMT_SMF.1/Base	X	Assignment performed.
FMT_SMR.1/Base	X	Selection performed.
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	Selection and Assignment performed.
FCS_CKM.2/Mobile_network	X	Assignment performed.
FCS_CKM.6/Mobile_network	X	Selection and Assignment performed.
FDP_ACC.2/FIREWALL		(A) Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A) Added from [PP-JCS].
FDP_IFC.1/JCVM		(A) Added from [PP-JCS].
FDP_IFF.1/JCVM		(A) Added from [PP-JCS].
FDP_RIP.1/OBJECTS		(A) Added from [PP-JCS].
FMT_MSA.1/JCRE		(A) Added from [PP-JCS].
FMT_MSA.1/JCVM		(A) Added from [PP-JCS].
FMT_MSA.2/FIREWALL_JCVM		(A) Added from [PP-JCS].
FMT_MSA.3/FIREWALL		(A) Added from [PP-JCS].
FMT_MSA.3/JCVM		(A) Added from [PP-JCS].

SFR	PP-eUICC	Security Target
FMT_SMF.1/RE		(A) Added from [PP-JCS]. Refined with iteration.
FMT_SMR.1/RE		(A) Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/ECC, FCS_CKM.1/Triple DES, FCS_CKM.1/AES		(A) Added from [PP-JCS]. Refined with iteration.
FCS_CKM.6/RE		(A) Added from [CC2]. Refined with iteration. Replaces FCS_CKM.4 from [PP-JCS].
FCS_COP.1/SHA FCS_COP.1/SIG_ECC FCS_COP.1/MAC_TDES FCS_COP.1/MAC_AES FCS_COP.1/CIPH_TDES FCS_COP.1/CIPH_AES FCS_COP.1/CIPH_AES_GCM FCS_COP.1/ECKA-EG		(A) Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A) Added from [PP-JCS].
FDP_RIP.1/APDU		(A) Added from [PP-JCS].
FDP_RIP.1/bArray		(A) Added from [PP-JCS].
FDP_RIP.1/GlobalArray		(A) Added from [PP-JCS].
FDP_RIP.1/KEYS		(A) Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A) Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A) Added from [PP-JCS].

SFR	PP-eUICC	Security Target
FAU_ARP.1		(A) Added from [PP-JCS].
FDP_SDI.2/DATA		(A) Added from [PP-JCS].
FPR_UNO.1		(A) Added from [PP-JCS].
FPT_FLS.1/RE		(A) Added from [PP-JCS]. Refined with iteration.
FPT_TDC.1/RE		(A) Added from [PP-JCS]. Refined with iteration.
FIA_ATD.1/AID		(A) Added from [PP-JCS].
FIA_UID.2/AID		(A) Added from [PP-JCS].
FIA_USB.1/AID		(A) Added from [PP-JCS].
FMT_MTD.1/JCRE		(A) Added from [PP-JCS].
FMT_MTD.3/JCRE		(A) Added from [PP-JCS].
FDP_ACC.2/ADEL		(A) Added from [PP-JCS].
FDP_ACF.1/ADEL		(A) Added from [PP-JCS].
FDP_RIP.1/ADEL		(A) Added from [PP-JCS].
FMT_MSA.1/ADEL		(A) Added from [PP-JCS].
FMT_MSA.3/ADEL		(A) Added from [PP-JCS].
FMT_SMF.1/ADEL		(A) Added from [PP-JCS].
FMT_SMR.1/ADEL		(A) Added from [PP-JCS].
FPT_FLS.1/ADEL		(A) Added from [PP-JCS].
FDP_RIP.1/ODEL		(A) Added from [PP-JCS].

SFR	PP-eUICC	Security Target
FPT_FLS.1/ODEL		(A) Added from [PP-JCS].
FAU_SAS.1		(A) Added to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added to cover O.IC.RE-COVERY.
FPT_RCV.4/OS		(A): Added to cover O.IC.SUP-PORT.
FPT_PHP.3		(A) Added to cover O.IC.SUP-PORT.
FIA_AFL.1/GP		(A): Added from [PP-GP]
FIA_UAU.1/GP		(A): Added from [PP-GP]
FIA_UAU.4/GP		(A): Added from [PP-GP]
FDP_UIT.1/GP		(A): Added from [PP-GP]
FDP_UCT.1/GP		(A): Added from [PP-GP]
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP]
FDP_IFC.2/GP-KL		(A): Added from [PP-GP]
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP]
FMT_MSA.3/GP		(A): Added from [PP-GP]
FMT_MSA.1/GP		(A): Added from [PP-GP]
FMT_SMR.1/GP		(A): Added from [PP-GP]. Re-finement of FDP_SMR.1/In-staller and FDP_SMR.1/CM.

SFR	PP-eUICC	Security Target
FPT_FLS.1/GP		(A): Added from [PP-GP]. Refinement of FPT_FLS.1/Installer.
FPT_RCV.3/GP		(A): Added from [PP-GP]. Refinement of FPT_RCV.3/Installer
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP]. Refinement of FDP_ITC.2/Installer.
FDP_ITC.2/GP-KL		(A): Added from [PP-GP]
FTP_ITC.1/GP		(A): Added from [PP-GP]
FDP_IFF.1/GP-KL		(A): Added from [PP-GP]
FMT_SMF.1/GP		(A): Added from [PP-GP]. Refinement performed.
FIA_UID.1/GP		(A): Added from [PP-GP]
FPT_TDC.1/GP		(A): Added from [PP-GP]
FCO_NRO.2/GP		(A): Added from [PP-GP]
FDP_ROL.1/GP		(A): Added from [PP-GP]
FDP_ACC.1/OS-UPDATE		(A): Added from [PP-GP]
FDP_ACF.1/OS-UPDATE		(A): Added from [PP-GP]
FMT_MSA.3/OS-UPDATE		(A): Added from [PP-GP]
FMT_SMR.1/OS-UPDATE		(A): Added from [PP-GP]

SFR	PP-eUICC	Security Target
FMT_SMF.1/OS-UPDATE		(A): Added from [PP-GP]
FIA_ATD.1/OS-UPDATE		(A): Added from [PP-GP]
FTP_TRP.1/OS-UPDATE		(A): Added from [PP-GP]
FCS_COP.1/OS-UPDATE-DEC		(A): Added from [PP-GP]
FCS_COP.1/OS-UPDATE-VER		(A): Added from [PP-GP]
FPT_FLS.1/OS-UPDATE		(A): Added from [PP-GP]

Table 10 Security Functional Requirement Consistency

2.5.3.10 SAR consistency

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

3. 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 TOE may face in the field, the assumptions on its operational environment, and the organizational policies that must be implemented by the TOE or within the operational environment.

3.1 Assets

The definition of the assets from [PP-eUICC], [PP-JCS] and [PP-GP] is not repeated here. See section 2.5.3.2 for the complete list is assets.

3.2 Users and Subjects

The definition of users and subjects from [PP-eUICC], [PP-JCS] and [PP-GP] is not repeated here. See section 2.5.3.3 for the complete list of users and subjects.

3.3 Threats

The definition of threats from [PP-eUICC] where no refinements are made is not repeated here. See section 2.5.3.4 for the complete list of threats.

Refined threats description is detailed in Table 11. The definition of each refined threat is present in [PP-eUICC]. The mapping against assets has been refined (the additional assets are underlined).

Threat	Directly threatened asset
T.UNAUTHORIZED-PROFILE-MNG	D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYs, D.APP_CODE, D.PIN
T.UNAUTHORIZED-PLATFORM-MNG	D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYs, D.APP_CODE
T.PROFILE-MNG-INTERCEPTION	D.MNO_KEYS, D.TSF_CODE (ISD-P and ISD-R), D.PROFILE_*, D.APP_C_DATA, D.APP_KEYs
T.PROFILE-MNG-ELIGIBILITY	D.TSF_CODE, D.DEVICE_INFO, D.EID, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYs, D.APP_CODE
T.UNAUTHORIZED-IDENTITY-MNG	D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, D.PK.EIM.ECDSA (SGP.32), D.APP_CODE, D.APP_I_DATA, D.APP_C_DATA, D.APP_KEYs, D.SEC_DATA
T.IDENTITY-INTERCEPTION	D.SECRETS, D.EID, D.PIN, D.APP_C_DATA, D.APP_KEYs
T.LOGICAL-ATTACK	D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_ RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, D.PIN, D.JCS_CODE, D.JCS_DATA, D.APP_CODE, D.API_DATA, D.SEC_DATA, D.CRYPTO, D.APP_I_DATA, D.APP_C_DATA, D.APP_KEYs

Table 11 Refined Threats

3.4 Organisational Security Policies

The definition of organizational security policies from [PP-eUICC] and [PP-JCS] is not repeated here. See section 2.5.3.5 for the complete list of OSPs.

3.5 Assumptions

The definition of Assumptions from [PP-eUICC] and [PP-JCS] is not repeated here. See section 2.5.3.6 for the complete list of Assumptions.

4. Security Objectives

4.1 Security objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] and [PP-JCS] are not repeated here. See section 2.5.3.7 for complete list is Security Objectives for the TOE.

Some objectives from the environment have been converted to objectives of the TOE, specifically the ones from [PP-eUICC] related to OE.RE* and OE.IC*. The replaced objectives from 2.5.3.7 and their description are listed next:

Security Objectives for the TOE	Description
O.IC.PROOF_OF_IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: (1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification). (2) It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PRE, S.PPI, and S.TELECOM). (3) It allows the S.PRE, S.PPI, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending

	on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection). (4) It provides a means to perform memory operations atomically for S.PRE, S.PPI, and S.TELECOM.
O.IC.RECOVERY	If there is a loss of power while an operation is in progress, the underlying IC must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.
O.RE.PRE-PPI	The Runtime Environment shall provide secure means for card management activities, including: o load of a package file, o installation of a package file, o extradition of a package file or an application, o personalization of an application or a Security Domain, o deletion of a package file or an application, o privileges update of an application or a Security Domain, o access to an application outside of its expected availability.
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.

O.RE.API	The Runtime Environment shall ensure that native code can be invoked only via an API.
O.RE.DATA-CONFIDENTIALITY	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
O.RE.IDENTITY	The Runtime Environment shall ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.

4.2 Security objectives for the operational environment

The list and definitions of the Security Objectives for the TOE from [PP-eUICC], 4.2 and A.3.2, and [PP-JCS] are not repeated here. See section 2.5.3.8 for complete list is Security Objectives for the Operational Environment.

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG This threat is covered by requiring authentication and authorization from the legitimate actors:

- O.PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP+ and MNO OTA Platform) will access the Security Domains functions and content;
- OE.SM-DP+ and OE.MNO protect the corresponding credentials when used offcard.

The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY). The authentication is supported by corresponding secure channels:

- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication with SM-DP+ and a secure channel for communication with MNO OTA Platform. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

Since the MNO-SD Security Domain is not part of the TOE, the operational environment has to guarantee that it will use securely the SCP80/81 secure channel provided by the TOE (OE.MNO-SD). In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required:

- compliance to security guidelines for applications (OE.APPLICATIONS and OE.CODE-EVIDENCE).

T.UNAUTHORIZED-PLATFORM-MNG This threat is covered by requiring authentication and authorization from the legitimate actors:

- O.PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.
- OE.SM-DP+ and OE.EIM (SGP.32) protect the corresponding credentials when used off- card.

The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY).

In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required:

- compliance to security guidelines for applications (OE.APPLICATIONS and OE.CODE-EVIDENCE).

T.PROFILE-MNG-INTERCEPTION Commands and profiles are transmitted by the SM-DP+ to its on-card representative (ISD-P), while profile data (including meta-data such as PPRs) is also transmitted by the MNO OTA Platform to its on-card representative (MNO-SD) by means of RPM requests from Profile owner to ISD-R (UpdateMetadataRequest), or by means of PSMO commands from eIM to ISD-R (SGP.32).

Consequently, the TSF ensures:

- Security of the transmission to the Security Domain (O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS) by requiring authentication from SM-DP+ and MNO OTA Platforms, and protecting the transmission from unauthorized disclosure, modification and replay. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

Since the MNO-SD Security Domain is not part of the TOE, the operational environment has to guarantee that it will securely use the SCP80/81 secure channel provided by the TOE (OE.MNO-SD).

OE.SM-DP+, OE.MNO and OE.EIM (SGP.32) ensure that the credentials related to the secure channels will not be disclosed when used by off-card actors.

T.PROFILE-MNG-ELIGIBILITY Device Info and eUICCInfo2, transmitted by the eUICC to the SM-DP+, are used by the SM-DP+ to perform the Eligibility Check prior to allowing profile download onto the eUICC.

Consequently, the TSF ensures:

- Security of the transmission to the Security Domain (O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS) by requiring authentication from SM-DP+, and protecting the transmission from unauthorized disclosure, modification and replay. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

OE.SM-DP+ ensures that the credentials related to the secure channels will not be disclosed when used by off-card actors.

O.DATA-INTEGRITY and O.RE.DATA-INTEGRITY ensure that the integrity of Device Info and eUICCInfo2 is protected at the eUICC level.

4.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG O.PPE-PPI and O.eUICC-DOMAIN-RIGHTS covers this threat by providing an access control policy for ECASD content and functionality.

The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY).

O.RE.IDENTITY ensures that at the Java Card level, the applications cannot impersonate other actors or modify their privileges.

T.IDENTITY-INTERCEPTION O.INTERNAL-SECURE-CHANNELS ensures the secure transmission of the shared secrets from the ECASD to ISD-R and ISD-P. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

OE.CI ensures that the CI root will manage securely its credentials off-card.

4.3.1.3 eUICC cloning

T.UNAUTHORIZED-eUICC O.PROOF_OF_IDENTITY guarantees that the off-card actor can be provided with a cryptographic proof of identity based on an EID.

O.PROOF_OF_IDENTITY guarantees this EID uniqueness by basing it on the eUICC hardware identification (which is unique due to O.IC.PROOF_OF_IDENTITY).

4.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT OE.TRUSTED-PATHS-LPAd-IPAd ensures that:

- the interfaces ES10a, ES10b and ES10c are trusted paths to the LPAd. (SGP.22)
- the interfaces ES10a and ES10b are trusted paths to IPAd. (SGP.32)

4.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS The objective O.ALGORITHMS ensures that a profile may only access the mobile network using a secure authentication method, which prevents impersonation by an attacker.

4.3.1.6 Second Level Threats

T.LOGICAL-ATTACK This threat is covered by controlling the information flow between Security Domains and the PPE, PPI, the Telecom Framework or any native/OS part of the TOE. As such it is covered:

- by the APIs provided by the Runtime Environment (O.RE.API);
- by the APIs of the TSF (O.API); the APIs of Telecom Framework, PPE and PPI shall ensure atomic transactions (O.IC.SUPPORT).

Whenever sensitive data of the TOE are processed by applications, confidentiality and integrity must be protected at all times by the Runtime Environment (O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY). However these sensitive data are also processed by the PPE, PPI and the Telecom Framework, which are not protected by these mechanisms. Consequently,

- the TOE itself must ensure the correct operation of PPE, PPI and Telecom Framework (O.OPERATE), and
- PPE, PPI and Telecom Framework must protect the confidentiality and integrity of the sensitive data they process, while applications must use the protection mechanisms provided by the Runtime Environment (O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY).

The following objectives for the operational environment are also required:

- prevention of unauthorized code execution by applications (O.RE.CODE-EXE),
- compliance to security guidelines for applications (OE.APPLICATIONS and OE.CODE-EVIDENCE).

T.PHYSICAL-ATTACK This threat is countered mainly by physical protections which rely on the underlying Platform and are therefore an environmental issue.

The security objectives O.IC.SUPPORT and O.IC.RECOVERY protect sensitive assets of the Platform against loss of integrity and confidentiality and especially ensure the TSFs cannot be bypassed or altered.

In particular, the security objective O.IC.SUPPORT provides functionality to ensure atomicity of sensitive operations, secure low level access control and protection against bypassing of the security features of the TOE. In particular, it explicitly ensures the independent protection in integrity of the Platform data.

Since the TOE cannot only rely on the IC protection measures, the TOE shall enforce any necessary mechanism to ensure resistance against side channels (O.DATA-CONFIDENTIALITY). For the same reason, the Java Card Platform security architecture must cover side channels (O.RE.DATA-CONFIDENTIALITY).

4.3.1.7 OS Update

T.CONFID-UPDATE-IMAGE.LOAD

O.CONFID-UPDATE-IMAGE.LOAD Counters the threat by ensuring the confidentiality of D.UPDATE_IMAGE during installing it on the TOE.

OE.CONFID-UPDATE-IMAGE.CREATE Counters the threat by ensuring that the D.UPDATE_IMAGE is not transferred in plain and that the keys are kept secret.

T.INTEG-UPDATE-IMAGE.LOAD

O.SECURE_LOAD_ACODE Counters the threat directly by ensuring the authenticity and integrity of D.UPDATE_IMAGE.

T.UNAUTH-UPDATE-IMAGE.LOAD

O.SECURE_LOAD_ACODE Counters the threat directly by ensuring that only authorized (allowed version) images can be installed.

O.AUTH-LOAD-UPDATE-IMAGE Counters the threat directly by ensuring that only authorized (allowed version) images can be loaded.

T.INTERRUPT_OSU

O.SECURE_LOAD_ACODE Counters the threat directly by ensuring that the TOE remains in a secure state after interruption of the OS Update procedure (Load Phase).

O.TOE_IDENTIFICATION Counters the threat directly by ensuring that D.TOE_IDENTIFICATION is only updated after successful OS Update procedure.

O.SECURE_AC_ACTIVATION Counters the threat directly by ensuring that the update OS is only activated after successful (atomic) OS Update procedure.

4.3.2 Organisational Security Policies

The OSP defined is OSP.LIFE-CYCLE as in [PP-eUICC].

4.3.3 Assumptions

The assumptions A.TRUSTED-PATHS-LPAd-IPAd, A.ACTORS and A.APPLICATIONS are defined as in [PP-eUICC]. A.CAP_FILE is defined as in [PP-JCS] section 5.4.

4.3.4 Rationale Tables

4.3.4.1 Threats and Security Objectives

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY,	Section 4.3.1.1

	O.RE.DATA-INTEGRITY, OE.MNO-SD	
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.EIM (SGP.32)	Section 4.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD, OE.EIM (SGP.32)	Section 4.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+, O.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 4.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 4.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 4.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 4.3.1.3

T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 4.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 4.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 4.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 4.3.1.6
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATE-IMAGE.LOAD, OE.CONFID-UPDATE-IMAGE.CREATE	Section 4.3.1.7

T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE, O.AUTH-LOAD-UPDATE-IMAGE	Section 4.3.1.7
T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE	Section 4.3.1.7
T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE, O.TOE_IDENTIFICATION, O.SECURE_AC_ACTIVATION	Section 4.3.1.7

Table 12 Threats and Security Objectives Coverage

Security Objectives	**Threats**
O.PPE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF-OF-IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK

O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DP+	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
O.EIM (SGP.32)	T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION
O.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.IC.RECOVERY	T.PHYSICAL-ATTACK
O.RE.PRE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG,

	T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UN-AUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd-IPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
O.SECURE_LOAD_ACODE	T.INTEG-UPDATE-IMAGE.LOAD, T.UNAUTH-UPDATE-IMAGE.LOAD, T.INTERRUPT_OSU
O.SECURE_AC_ACTIVATION	T.INTERRUPT_OSU
O.TOE_IDENTIFICATION	T.INTERRUPT_OSU
O.CONFID-UPDATE-IMAGE.LOAD	T.CONFID-UPDATE-IMAGE.LOAD
O.AUTH-LOAD-UPDATE-IMAGE	T.UNAUTH-UPDATE-IMAGE.LOAD

OE.CONFID_UPDATE_IMAGE.CRE-ATE	T.CONFID-UPDATE-IMAGE.LOAD

Table 13 Security Objectives and Threats – Coverage

4.3.4.2 OSPs and Security Objectives

Organisational Security Policies	**Security Objective**	**Rationale**
OSP.LIFE-CYCLE	O.PPE-PPI, O.RE.PRE-PPI, O.OPERATE	[PP-eUICC], Section 4.3.2

Table 14 OSPs and Security Objectives – Coverage

Security Objectives	**Organisational Security Policies**
O.PPE-PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF-OF-IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	

OE.SM-DP+	
OE.MNO	
OE.EIM (SGP.32)	
O.IC.PROOF_OF_IDENTITY	
O.IC.SUPPORT	
O.IC.RECOVERY	
O.RE.PRE-PPI	OSP.LIFE-CYCLE
O.RE.SECURE-COMM	
O.RE.API	
O.RE.DATA-CONFIDENTIALITY	
O.RE.DATA-INTEGRITY	
O.RE.IDENTITY	
O.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd-IPAd	
OE.APPLICATIONS	
OE.MNO-SD	
OE.SM-DS	
O.SECURE_LOAD_ACODE	
O.SECURE_AC_ACTIVATION	
O.TOE_IDENTIFICATION	
O.CONFID-UPDATE-IMAGE.LOAD	
O.AUTH-LOAD-UPDATE-IMAGE	

OE.CONFID_UPDATE_IMAGE.CREATE	

Table 15 Security Objectives and OSPs – Coverage

4.3.4.3 Assumptions and Security Objectives for the Operational Environment

Assumptions	**Security Objectives for the Operational Environment**	**Rationale**
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd-IPAd	[PP-eUICC], section 4.3.3
A.ACTORS	OE.CI, OE.SM-DP+, OE.MNO, OE.EIM (SGP.32), OE.SM-DS	[PP-eUICC], section 4.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	[PP-eUICC], section 4.3.3
A.CAP_FILE	OE.CAP_FILE	[PP-JCS], section 6.3.3

Table 16 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	**Assumptions**
OE.CI	A.ACTORS
OE.SM-DP+	A.ACTORS
OE.MNO	A.ACTORS
OE.SM-DS	A.ACTORS
OE.TRUSTED-PATHS-LPAd-IPAd	A.TRUSTED-PATHS-LPAd-IPAd
OE.MNO-SD	

OE.EIM (SGP.32)	A.ACTORS
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.CAP_FILE	A.CAP_FILE
OE.CONFID_UPDATE_IMAGE.CREATE	

Table 17 Security Objectives for the Operational Environment and Assumptions – Coverage

5. Extended Requirements

The following components are defined in the current Security Target:

- Extended Family FAU_SAS – Audit Data Storage

FAU_SAS.1 definition has been taken from [PP-0084] section 5.3 with no modification.

6. Security Requirements

The following SFRs are relevant for this TOE.

SFR	Included in this ST
[PP-eUICC] SFRs	All SFRs of base PP, section 6.1.
[PP-JCS] SFRs	All SFRs listed in section 2.5.3.9, added for secure RE support.
FPT_PHP.3	Added for secure IC support.
[PP-GP] SFRs	Added for Card Content Management.
OS Update SFRs	Added for secure post-issuance updates (ITL) support.

Table 18 SFRs of the TOE of this ST

The following subsections contain the Security Functional Requirements applicable to both configurations of the TOE at the same time: [SGP.22] and [SGP.32]. However, the operations may not be the same for both configurations.

In cases where the operations are specific to one configuration, this is indicated by referencing the specification in brackets: (SGP.22) or (SGP.32). See for example the selection in FIA_USB.1/EXT SFR.

In cases where there is no specification referenced, the operation applies to both configurations. See for example the assignment in FIA_UID.1.1/EXT SFR.

Note: this criteria is applicable to assignments, selections and application notes.

6.1 eUICC Security Functional Requirements

6.1.1 Introduction

The introduction and security attributes definition are present in [PP-eUICC] section 6.1, and are not repeated here.

6.1.2 Identification and authentication

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **[assignment: *none*]**[1].

on behalf of the user to be performed before the user is identified.

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

Application note 1:

This SFR is related to the identification of the following external (remote) users of the TOE:

- *U.SM-DP+;*
- *U.MNO-OTA;*
- *U.EIM (SGP.32).*

The identification of the only local user (U.MNO-SD) is addressed by the FIA_UID.1/MNO-SD SFR.

Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user

FIA_UAU.1/EXT Timing of authentication

FIA_UAU.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **user identification**
- **[assignment: *none*]**[2].

on behalf of the user to be performed before the user is authenticated.

---

[1] [assignment: *list of additional TSF mediated actions*]
[2] [assignment: *list of additional TSF mediated actions*]

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

Application note 2:

This SFR is related to the authentication of the following external (remote) users of the TOE:

- *U.SM-DP+;*
- *U.MNO-OTA;*
- *U.EIM (SGP.32).*

As the cryptographic mechanisms used for the authentication may be provided by the underlying Platform. This ST includes the corresponding FCS_COP.1 SFRs to cover the requirements stated by [SGP.22]:

- *A U.SM-DP+ must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.DPauth.ECDSA and CERT.DPpb.ECDSA), as well as the public key of the CI (D.PK.CI.ECDSA).*
- *U.MNO-OTA must be authenticated using a SCP80 secure channel according to [TS102 225] and [TS102 226] using the parameters defined in [SGP.02] section 2.4.3, or optionally SCP81 according to [GP AM B] using the parameters defined in [SGP.02] section 2.4.4 (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO).*
- *U.EIM must be authenticated by verifying its ECDSA signature using the public key PK.EIM.ECDSA included in its certificate (CERT.EIM.ECDSA).*

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with at least one of the elliptic curves referenced for that purpose in [SGP.22] and/or [SGP.32].

FIA_USB.1/EXT User-subject binding

FIA_USB.1.1/EXT The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **SM-DP+ OID is associated to S.ISD-R, acting on behalf of U.SM-DP+;**
- **MNO OID is associated to U.MNO-SD, acting on behalf of U.MNO-OTA;**
- **SM-DS OID is associated to S.ISD-R, acting on behalf of U.SM-DS;**
- **[selection:**
  - ***eIM ID is associated to S.ISD-R, acting on behalf of U.EIM (SGP.32),***
  - ***no other associations (SGP.22)*]**[3]**.**

FIA_USB.1.2/EXT The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- **Initial association of SM-DP+ OID and MNO OID requires U.SM-DP+ to be authenticated via "CERT.DPauth.ECDSA";**
- **Initial association of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA";**
- **[selection:**
  - ***Initial association of eIM ID requires U.EIM to be authenticated via CERT.EIM.ECDSA (SGP.32),***
  - ***no other initial associations (SGP.22)].***[4]

FIA_USB.1.3/EXT The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

- **change of SM-DP+ OID requires U.SM-DP+ to be authenticated via "CERT.DPauth.ECDSA";**
- **change of MNO OID is not allowed;**

[3] [selection: eIM ID is associated to S.ISD-R, acting on behalf of U.EIM, no other associations]
[4] [selection: Initial association of eIM ID requires U.EIM to be authenticated via CERT.EIM.ECDSA (SGP.32), no other initial associations].

- **change of SM-DS OID requires U.SM-DS to be authenticated via “CERT.DSauth.ECDSA”;**
- **[selection:**
  - ***change of eIM ID requires U.EIM to be authenticated via “CERT.EIM.ECDSA (SGP.32),***
  - ***no other changes (SGP.22)].*** [5]

Application note 3:

This SFR is related to the binding of external (remote) users to local subjects or users of the TOE:

- *U.SM-DP+ binds to a subject (S.ISD-R);*
- *U.SM-DS binds to a subject (S.ISD-R)*
- *U.MNO-OTA binds to an on-card user (U.MNO-SD);*
- *U.EIM binds to a subject (S.ISD-R).*

U.MNO-SD is not a subject of the TOE, but an external on-card user acting on behalf of U.MNO-OTA, which is an external off-card user.
This SFR is related to the following commands:

- *Initial association of the D.MNO_KEYS keyset is performed by the ES8+.ConfigureISDP command.*

FIA_UAU.4/EXT Single-use authentication mechanisms

FIA_UAU.4.1/EXT The TSF shall prevent reuse of authentication data related to **the authentication mechanism used to open a secure communication channel between the eUICC and**

- **U.SM-DP+**
- **U.MNO-OTA**
- **[Selection:**
  - ***none (SGP.22),***
  - ***U.EIM (SGP.32)*]**[6]

[5] [selection: change of eIM ID requires U.EIM to be authenticated via “CERT.EIM.ECDSA (SGP.32), no other changes].
[6] [Selection: none, U.EIM (SGP.32)]

Application note 4:

This SFR is related to the authentication of external (remote) users of the TOE:

- *U.SM-DP+;*
- *U.MNO-OTA;*
- *U.EIM (SGP.32).*

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow **[assignment: *application selection, requesting data that identifies the eUICC*]**[7] on behalf of the user to be performed before the user is identified.

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

Application note 5:

This SFR is related to the identification of the local user U.MNO-SD only. The identification of remote users is addressed by the FIA_UID.1/EXT SFR.

It should be noted that the U.MNO-SD is identified but not authenticated. However, U.MNO-SD is installed on the TOE by the U.SM-DP+ via the subject S.ISD-R (see FDP_ACF.1/ISDR), and the binding between U.SM-DP+ and S.ISD-R requires authentication of U.SM-DP+, as described in FIA_USB.1/EXT.

FIA_USB.1/MNO-SD User-subject binding

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

[7] [assignment: *list of TSF-mediated actions*]

FIA_ATD.1/Base User attribute definition

FIA_ATD.1.1/Base The TSF shall maintain the following list of security attributes belonging to individual users:

- **CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-DP+;**
- **MNO OID belonging to U.MNO-OTA;**
- **AID belonging to U.MNO-SD;**
- **CERT.DSauth.ECDSA and SM-DS OID belonging to U.SM-DS;**
- **[selection:**
    - ***CERT.EIM.ECDSA and eIM ID belonging to U.EIM (SGP.32),***
    - ***no additional attributes (SGP.22)]*** [8]

FIA_API.1 Authentication Proof of Identity

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

6.1.3 Communication

FDP_IFC.1/SCP Subset information flow control

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FDP_IFF.1/SCP Simple security attributes

FDP_IFF.1.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** based on the following types of subject and information security attributes:

[8] [selection: CERT.EIM.ECDSA and eIM ID belonging to U.EIM, no additional attributes].

- **users/subjects/objects:**
  - **U.SM-DP+, SO.ISD-P and SO.ISD-R, with security attribute D.SECRETS**
  - **U.MNO-OTA and U.MNO-SD, with security attribute D.MNO_KEYS**
- **information: transmission of commands**.

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

- **The TOE shall permit communication between U.MNO-OTA and U.MNO- SD in a SCP80 or SCP81 secure channel.**

FDP_IFF.1.3/SCP The TSF shall enforce **[assignment: *no additional information flow control SFP rules*]**[9].

FDP_IFF.1.4/SCP The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[10].

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

- **The TOE shall reject communication between U.SM-DP+ and S.ISD-R if it is not performed in a SCP-SGP22 secure channel.**

Application note 6:

More details on the secure channels can be found in [SGP.22]

- For SM-DP+: Section 5.5
- For MNO-SD: Section 5.4

FTP_ITC.1/SCP Inter-TSF trusted channel

---

[9] [assignment: *additional information flow control SFP rules*]
[10] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

FTP_ITC.1.1/SCP 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/SCP The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/SCP The TSF shall initiate communication via the trusted channel for **[assignment:**

- ***the remote OTA platform via SCP80 or SCP81 secure channel to transmit ES6 functions (UpdateMetadata),***
- ***the SM-DP+ via SCP-SGP.22 secure channel to transmit the ES8+ functions (Profile Download and Installation)*]**[11].

Application note 7:

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this ST includes the corresponding FCS_COP.1 SFR to cover the requirements stated by [SGP.22] and [SGP.32]:

- *The secure channels to SM-DP+ must be SCP-SGP22 secure channels. Identification of endpoints is addressed by the use of AES according to [GP AM F] using the parameters defined in [SGP.22] and [SGP.32], sections 2.6 and 5.5.*
- *SCP80 must be provided to build secure channels to MNO OTA Platform (section 5.4 of [SGP.22] and [SGP.32]). The TSF may also permit to use a SCP81 secure channel to perform the same functions than the SCP80 secure channel.*

Related keys are:

- *either generated on-card (D.SECRETS); see FCS_CKM.1/SCP-SM for further details,*

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

- *or distributed along with the profile (D.MNO_KEYS); see FCS_CKM.2/SCP-MNO for further details.*

In terms of commands, the TSF shall permit remote actors to initiate communication via a trusted channel in the following cases:

- *The TSF shall permit the SM-DP+ to open a SCP-SGP22 secure channel to transmit the following operations:*
  - *ES8+.InitialiseSecureChannel*
  - *ES8+.ConfigureISDP*
  - *ES8+.StoreMetadata*
  - *ES8+.ReplaceSessionKeys*
  - *ES8+.LoadProfileElements.*
- *The TSF shall permit the LPAd/IPAd to transmit the following operations:*
  - *ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.5)*
  - *ES10a.SetDefaultDpAddress (SGP.22)*
  - *ES10b.SetDefaultDpAddress (SGP.32)*
  - *ES10b.PrepareDownload*
  - *ES10b.LoadBoundProfilePackage*
  - *ES10b.GetEUICCChallenge*
  - *ES10b.GetEUICCInfo*
  - *ES10b.ListNotification*
  - *ES10b.RetrieveNotificationsList*
  - *ES10b.RemoveNotificationFromList*
  - *ES10b.AuthenticateServer*
  - *ES10b.CancelSession*
  - *ES10b.LoadEuiccPackage (SGP.32)*
  - *ES10b.AddInitialEim (SGP.32)*
  - *ES10b.GetCerts (SGP.32)*
  - *ES10b.ImmediateEnable (SGP.32)*
  - *ES10b.ProfileRollback (SGP.32)*
  - *ES10b.ConfigureImmediateProfileEnabling (SGP.32)*
  - *ES10b.GetEimConfigurationData (SGP.32)*
  - *ES10b.GetProfilesInfo (SGP.32)*

  - *ES10c.GetProfilesInfo (SGP.22)*
  - *ES10c.EnableProfile (SGP.22)*
  - *ES10c.DisableProfile (SGP.22)*
  - *ES10c.DeleteProfile (SGP.22)*
  - *ES10c.eUICCMemoryReset (SGP.22)*
  - *ES10b.GetEID (SGP.32)*
  - *ES10c.GetEID (SGP.22)*
  - *ES10c.SetNickname (SGP.22)*
  - *ES10b.GetRAT*
- *The TSF may permit the LPAd/IPAd to transmit the following operations:*
  - *ES10b.LoadCRL (SGP.22 v2.5)*
  - *ES10b.eUICCMemoryReset (SGP.32)*
  - *ES10b.ExecuteFallbackMechanism (SGP.32)*
  - *ES10b.ReturnFromFallback (SGP.32)*
  - *ES10b.EnableEmergencyProfile (SGP.32)*
  - *ES10b.DisableEmergencyProfile (SGP.32)*
  - *ES10b.GetConnectivityParameters*
- *The TSF shall permit the remote OTA Platform to open a SCP80 or SCP81 secure channel to transmit the following operation:*
  - *ES6.UpdateMetadata.*

FDP_ITC.2/SCP Import of user data with security attributes

FDP_ITC.2.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/SCP 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/SCP 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/SCP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: *none*]**[12].

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

FPT_TDC.1.1/SCP The TSF shall provide the capability to consistently interpret

- **Commands from U.SM-DP+ and U.MNO-OTA**
- **Downloaded objects from U.SM-DP+ and U.MNO-OTA**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SCP The TSF shall use **[assignment: *the following interpretation rules:***

- **(SGP.22)**
  - ***[SGP.22] §5.4.1 for commands and downloaded objects from U.MNO-OTA***
  - ***[SGP.22] §5.5.1-5.5.5 for commands and downloaded objects from U.SM-DP+***
  - ***[SGP.22] §5.7.3-5.7.22 for LPAd commands***
- ***(SGP.32):***
  - ***[SGP.32] §5.4 for commands and downloaded objects from U.MNO-OTA***
  - ***[SGP.32] §5.5 for commands and downloaded objects from U.SM-DP+***
  - ***[SGP.32] §5.8, §5.9 and §5.13 for IPAd commands*]**[13]

[12] [assignment: *additional importation control rules*]
[13] [assignment: *list of interpretation rules to be applied by the TSF*]

when interpreting the TSF data from another trusted IT product.

Application note 8:

The commands related to the SFRs FPT_TDC.1/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP and the Downloaded objects related to this SFR FPT_TDC.1/SCP are listed below:

- SM-DP+ commands
    - ES8+.InitialiseSecureChannel
    - ES8+.ConfigureISDP
    - ES8+.StoreMetadata
    - ES8+.ReplaceSessionKeys
    - ES8+.LoadProfileElements
- LPAd/IPAd commands
    - ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.5)
    - ES10a.SetDefaultDpAddress (SGP.22)
    - ES10b.SetDefaultDpAddress (SGP.32)
    - ES10b.PrepareDownload
    - ES10b.LoadBoundProfilePackage
    - ES10b.GetEUICCChallenge
    - ES10b.GetEUICCInfo
    - ES10b.ListNotification
    - ES10b.RetrieveNotificationsList
    - ES10b.RemoveNotificationFromList
    - ES10b.LoadCRL (SGP.22 v2.5)
    - ES10b.AuthenticateServer
    - ES10b.CancelSession
    - ES10b.LoadEuiccPackage (SGP.32)
    - ES10b.AddInitialEim (SGP.32)
    - ES10b.GetCerts (SGP.32)
    - ES10b.ImmediateEnable (SGP.32)
    - ES10b.ProfileRollback (SGP.32)
    - ES10b.ConfigureAutomaticProfileEnabling (SGP.32)
    - ES10b.GetEimConfigurationData (SGP.32)
    - ES10b.GetProfilesInfo (SGP.32)
    - ES10c.GetProfilesInfo (SGP.22)
    - ES10c.EnableProfile
    - ES10c.DisableProfile
    - ES10c.DeleteProfile

  - ES10b.eUICCMemoryReset (SGP.32)
  - ES10c.eUICCMemoryReset (SGP.22)
  - ES10b.GetEID (SGP.32)
  - ES10c.GetEID (SGP.22)
  - ES10c.SetNickname (SGP.22)
  - ES10b.GetRAT
  - ES10b.ExecuteFallbackMechanism (SGP.32)
  - ES10b.ReturnFromFallback (SGP.32)
  - ES10b.EnableEmergencyProfile (SGP.32)
  - ES10b.DisableEmergencyProfile (SGP.32)
  - ES10b.GetConnectivityParameters (SGP.32)
- Downloaded objects from SM-DP+
  - Session keys
  - Profile Metadata (including PPR data)
- MNO commands
  - ES6.UpdateMetadata

FDP_UCT.1/SCP Basic data exchange confidentiality

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FDP_UIT.1/SCP Data exchange confidentiality

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FCS_CKM.1/SCP-SM Cryptographic key generation

FCS_CKM.1.1/SCP-SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curves Key agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following: **[assignment: *NIST P-256 and brainpoolP256r1*]**[14]

Application note 9:

This key generation mechanism is used to generate

- *D.SECRETS keyset via the ES8+.InitialiseSecureChannel command, using the U.SM-DP+ public key PK.DP.ECKA.*

[14] [assignment: at least one elliptic curve referenced in [SGP.22] and/or [SGP.32]]

The Elliptic Curve cryptography used for this key agreement may be provided by the underlying Platform and covered by the FCS_COP.1 SFR.

FCS_CKM.2/SCP-MNO Cryptographic key distribution

FCS_CKM.2.1/SCP-MNO The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[assignment: *PUT KEY, STORE DATA LoadBoundProfilePackage*]**[15] that meets the following: **[assignment: *[GP] §11.8 §11.11, [SGP.22] §5.7.6 and [SGP.32] §5.9.8*]**[16].

Application note 10:

This SFR is related to the distribution of

- *D.MNO_KEYS during profile download.*

Note: this SFR does not apply to the private keys loaded pre-issuance of the TOE (D.SK.EUICC.ECDSA).

FCS_CKM.6/SCP-SM Cryptographic key destruction

FCS_CKM.6.1/SCP-SM The TSF shall destroy **D.SECRETS, CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DSauth.ECDSA, D.CERT.EUICC.ECDSA, D.SK.EUICC.ECDSA and D.PK.CI.ECDSA** when **[selection: *no longer needed*][17].**

FCS_CKM.6.2/SCP-SM The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-SM in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values*][18]** that meets the following: **[assignment: *none*]**[19].

---

[15] [assignment: *key distribution method*]
[16] [assignment: *list of standards*]
[17] [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]]
[18] [assignment: cryptographic key destruction method]
[19] [assignment: list of standards]

FCS_CKM.6/SCP-MNO Cryptographic key destruction

FCS_CKM.6.1/SCP-MNO The TSF shall destroy **D.MNO_KEYS** when **[selection: *no longer needed*][20].**

FCS_CKM.6.2/SCP-MNO The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-SM in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values*][21]** that meets the following: **[assignment: *none*]**[22].

6.1.4 Security Domains

FDP_ACC.1/ISDR Subset access control

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FDP_ACF.1/ISDR Security attribute based access control

FDP_ACF.1.1/ISDR The TSF shall enforce the **ISD-R access control SFP** to objects based on the following:

- **subjects: S.ISD-R**
- **objects:**
  - **SO.ISD-P with security attributes "state" "PPR", and [Selection: *no additional attributes*][23]**
- **operations:**
  - **create and configure profile**
  - **Store profile metadata**
  - **Enable profile**

[20] [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction*]]
[21] [assignment: *cryptographic key destruction method*]
[22] [assignment: *list of standards*]
[23] [Selection: "Reference Enterprise Rule" (SGP.22 v3.1 or higher), no additional attributes]

- **Disable profile**
- **Delete profile**
- **Perform a Memory reset.**

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

- **Enabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "DISABLED" and**
  - **in case a currently enabled S.ISD-P has to be disabled, the PPR data of this S.ISD-P allows its disabling, and**
  - **[Selection: *no additional conditions*]**[24]
- **Disabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "ENABLED" and**
  - **the corresponding S.ISD-P's PPR data allows its disabling.**
- **Deleting a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is not in the state "ENABLED" and**
  - **the corresponding S.ISD-P's PPR data allows its deletion.**
- **Performing a S.ISD-P Memory reset is authorized regardless of the involved S.ISD-P's state or PPR attribute.**

FDP_ACF.1.3/ISDR The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *none*]**[25].
FDP_ACF.1.4/ISDR The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: *none*]**[26].

---

[24] [Selection: the Reference Enterprise Rule allows enabling S.ISD-P (SGP.22 v3.1 or higher), no additional conditions]
[25] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[26] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Application note 11:

This policy describes the rules to be applied to access Platform Management or eUICC Management operations. It covers the access to the following operations by ISD-R required by sections 5.x of [SGP.22] and/or [SGP.32]:

- *ES8+.ConfigureISDP (Create and configure profile)*
- *ES8+.StoreMetadata (Store profile metadata)*
- *ES10c.EnableProfile (Enable profile) (SGP.22)*
- *ES10c.DisableProfile (Disable profile) (SGP.22)*
- *ES10c.DeleteProfile (Delete profile) (SGP.22)*
- *ES10c.eUICCMemoryReset (Perform a Memory reset) (SGP.22)*
- *ES10b.eUICCMemoryReset (Perform a Memory reset)*
- *ES10b.ImmediateEnable (Enable Profile)*
- *ES10b.ProfileRollback (Enable Rollback profile)*
- *ES10b.ExecuteFallbackMechanism (Enable Fallback profile)*
- *ES10b.EnableEmergencyProfile (Enable eCall Profile)*
- *ES10b.DisableEmergencyProfile (Disable eCall Profile)*
- *ESep.Enable (Enable profile) (SGP.32)*
- *ESep.Disable (Disable Profile) (SGP.32)*
- *ESep.Delete (Delete Profile) (SGP.32)*

FDP_ACC.1/ECASD Subset access control

FDP_ACC.1.1/ECASD The TSF shall enforce the **ECASD access control SFP** on

- **subjects: S.ISD-R, S.ECASD**
- **objects: data and attributes of ECASD,**
- **operations:**
  - **execution of a ECASD function**
  - **access to output data of these functions**
- **[assignment:**
  - ***(SGP.22) additional operations defined by the interfaces ES8+ (SM-DP+ – eUICC), and ES10x (LPA – eUICC), creation of an eUICC signature on material provided by an ISD-R***

- ***(SGP.32) additional operations defined by the interfaces ES8+ (SM-DP+ – eUICC), and ES10x (IPA – eUICC), creation of an eUICC signature on material provided by an ISD-R*]**[27]**.**

FDP_ACF.1/ECASD Security attribute based access control

FDP_ACF.1.1/ECASD The TSF shall enforce the **ECASD access control SFP** to objects based on the following:

- **subjects: S.ISD-R, with security attribute "AID", S.ECASD**
- **objects: data and attributes of S.ECASD**
- **operations:**
  - **execution of a ECASD function**
    - **Verification of the off-card entities Certificates (SM-DP+, SM-DS), provided by an ISD-R, with the eSIM CA public key (PK.CI.ECDSA)**
    - **Creation of an eUICC signature on material provided by an ISD-R**
- **access to output data of these functions**
- **[assignment: *none*][28].**

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

- **Authorized users: only S.ISD-R, identified by its AID, shall be authorized to execute the following S.ECASD functions:**
  - **Verification of a certificate CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, or CERT.DSauth.ECDSA provided by an ISD-R, with the eSIM CA public key (D.PK.CI.ECDSA)**
  - **Creation of an eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R**

---

[27] [assignment: *additional list of subjects, objects, and operations between subjects and objects covered by the SFP*]

[28] [assignment: *additional list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

- **[assignment:**
    - ***rules defined in [SGP.22], Section 2.4 and***
    - ***rules defined in [SGP.32], section 2.4*]**[29]**.**

FDP_ACF.1.3/ECASD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *none*]**[30].

FDP_ACF.1.4/ECASD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: *none*]**[31].

6.1.5 Platform Services

FDP_IFC.1/ Platform_services Subset information flow control

FDP_IFC.1.1/Platform_services The TSF shall enforce the **Platform services information flow control SFP** on

- **users/subjects:**
    - **S.ISD-R, S.ISD-P, U.MNO-SD**
    - **Platform code (S.PRE, S.PPI, S.TELECOM)**
- **information:**
    - **D.PROFILE_NAA_PARAMS**
    - **D.PROFILE_RULES**
    - **D.PLATFORM_RAT**
- **operations:**
    - **installation of a profile**
    - **PPR and RAT enforcement**
    - **network authentication.**
    - **[selection: *no additional operations*]**[32]

FDP_IFF.1/Platform_services Simple security attributes

---

[29] [assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[30] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[31] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[32] [selection: Reference Enterprise Rule enforcement (SGP.22 v3.1 or higher), no additional operations]

FDP_IFF.1.1/Platform_services The TSF shall enforce the **Platform services information flow control SFP** based on the following types of subject and information security attributes:

- **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"**
- **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_RULES**
  - **D.PLATFORM_RAT**
- **operations:**
  - **installation of a profile**
  - **PPR and RAT enforcement**
  - **network authentication.**
  - **[selection: *no additional operations*]**[33]

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

- **D.PROFILE_NAA_PARAMS shall be transmitted only:**
  - **by U.MNO-SD to S.TELECOM in order to execute the network authentication function**
  - **by S.ISD-R to S.PPI using the profile installation function**
- **D.PROFILE_RULES shall be transmitted only**
  - **by S.ISD-R to S.PRE in order to execute the PPR enforcement function**
  - **[selection: *no additional information flows*]**[34]
- **D.PLATFORM_RAT shall be transmitted only**
  - **by S.ISD-R to S.PRE in order to execute the RAT enforcement function.**

---

[33] [selection: Reference Enterprise Rule enforcement (SGP.22 v3.1 or higher), no additional operations]

[34] [selection: *by S.ISD-R to S.PRE in order to execute the Reference Enterprise Rule enforcement function (SGP.22 v3.1 or higher), no additional information flows*]

FDP_IFF.1.3/Platform_services The TSF shall enforce the **[assignment: *following additional information flow control SFP rules: none*]**[35].

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[36].

FDP_IFF.1.5/Platform_services The TSF shall explicitly deny an information flow based on the following rules: **[assignment: *when none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold*]**[37].

FPT_FLS.1/Platform_services Failure with preservation of secure state

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

- **failure that lead to a potential security violation during the processing of a S.PRE, S.PPI or S.TELECOM API specific functions:**
    - **Installation of a profile**
    - **PPR and RAT enforcement**
    - **Network authentication**
    - **[selection: *no additional functions*]**[38]
- **[assignment: *none*]**[39]**.**

6.1.6 Security management

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **[selection: *hybrid deterministic*]**[40] random number generator that implements: **[assignment:**

35 [assignment: *additional information flow control SFP rules*]
36 [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
37 [assignment: *rules, based on security attributes, that explicitly deny information flows*]
38 [selection: *Reference Enterprise Rule enforcement (SGP.22 v3.1 or higher), no additional functions*]
39 [assignment: *other type of failure*]
40 [selection: *deterministic, hybrid deterministic, physical, hybrid physical*]

(DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 as a random source.
(DRG.4.2) The RNG provides forward secrecy.
(DRG.4.3) The RNG provides backward secrecy, even if the current internal state is known.
(DRG.4.4) The RNG provides enhanced forward secrecy on condition: for every call.
***(DRG.4.5)The internal state of the RNG is seeded by a PTRNG of class PTG.2*]**[41]

FCS_RNG.1.2 The TSF shall provide **[selection: *octets of bits*]**[42] that meet**: [assignment:**

(DRG.4.6) The RNG generates output for which two strings of bit length 128 are mutually different with probability 1 - 2^128.

***(DRG.4.7) Statistical test suites cannot practically distinguish the random number from output sequences of an ideal RNG. The random numbers pass test procedure A and no additional test suites*]**[43].

Application note 12:

The TOE implements DRG.4 as defined in AIS20/31.

FPT_EMS.1/Base TOE Emanation of TSF and User data

FPT_EMS.1.1/Base The TOE shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in

ID	Emission	Attack surface	TSF data	User data
1	**[assignment: *information about IC power consumption,***	**Any**	**-**	**o D.SECRETS;** **o D.SK.EUICC.ECDSA** **and the secret keys which are part of the following keysets:**

[41] [assignment: *list of security capabilities of the selected RNG class*]
[42] [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
[43] [assignment: *a defined quality metric of the selected RNG class*]

	electromag-netic radia-tion, radio emission, in-ternal state transition and timing during com-mand execu-tion] in ex-cess of [as-signment: non-useful infor-mation][44]			**o D.MNO_KEYS,** **o D.PROFILE_NAA_PARAMS.**

Application note 13:

The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate from internal operation of the TOE or may originate from an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE.

Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, and so on.

FDP_SDI.1 Stored data integrity monitoring

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FDP_RIP.1/Base Subset residual information protection

[44] [assignment: list of types of emissions]

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FPT_FLS.1/Base Failure with preservation of secure state
The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FMT_MSA.1/PLATFORM_DATA Management of security attributes

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FMT_MSA.1/RULES Management of security attributes

FMT_MSA.1.1/RULES The TSF shall enforce the **Secure Channel protocol information flow control SFP** to restrict the ability to <u>change_default, query, modify and delete</u> the security attributes

- **D.PROFILE_RULES**

to

- **S.ISD-R for change_default, via function "ES8+.ConfigureISDP"**
- **S.ISD-R for query**
- **S.ISD-P for modify, via function "ES6.UpdateMetadata"**
- **[selection:**
  - ***S.ISD-R to delete, via function "ES10c.DeleteProfile" (SGP.22),***
  - ***S.ISD-R to delete, via function "ESep.Delete" (SGP.32)*]**[45]

FMT_MSA.1/CERT_KEYS Management of security attributes

FMT_MSA.1.1/CERT_KEYS The TSF shall enforce the **ECASD access control SFP** to restrict the ability to query and delete the security attributes

[45] [selection*: S.ISD-R to modify, via function "ES10b.LoadRPMPackage (UpdateMetadataRequest)" (SGP.22 v3.1 or higher), S.ISD-R to delete, via function "ES10c.DeleteProfile" (SGP.22), S.ISD-R to delete, via function "ESep.Delete" (SGP.32)*

- **D.CERT.EUICC.ECDSA**
- **D.PK.CI.ECDSA**
- **D.CERT.EUM.ECDSA**
- **D.MNO_KEYS**

to

- **S.ISD-R for: query D.PK.CI.ECDSA delete D.MNO_KEYS, via function [selection:**
  - **ES10c.DeleteProfile (SGP.22),**
  - **ESep.Delete (SGP.32)]**[46]
- **no actor for other operations**

Application note 14:

The modification of D.MNO_KEYS keysets is forbidden. To modify the keysets, one must delete the profile and load another profile.

FMT_SMF.1/Base Specification of Management Functions

FMT_SMF.1.1/Base The TSF shall be capable of performing the following management functions: **[assignment: *Profile Management functions specified in [SGP.22] and [SGP.32]]*** [47].

FMT_SMR.1/Base Security roles

FMT_SMR.1.1/Base The TSF shall maintain the roles

- **External users:**
  - **U.SM-DP+**
  - **U.MNO-SD**
  - **U.MNO-OTA**
  - **U.SM-DS**
  - **[selection: *U.EIM (SGP.32)*]**[48]
- **Subjects:**
  - **S.ISD-R**

[46] [selection: *ES10c.DeleteProfile (SGP.22), ESep.Delete (SGP.32)*]
[47] [assignment: *list of management functions to be provided by the TSF*]
[48] [selection: *U.EIM (SGP.32)*]

- **S.ISD-P**
- **S.ECASD**
- **S.PPI**
- **S.PRE**
- **S.TELECOM.**

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

Application note 15:

The roles defined here correspond to the users and subjects defined in Section 3.2.

Note that [PP-eUICC] does not include SGP.22 in the selection from FMT_SMR.1/Base. To make this selection correctly, the correct operation is:

- *U.EIM (SGP.32)*
- *None (SGP.22)*

FMT_MSA.1/RAT Management of security attributes

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

FMT_MSA.3 Static attribute initialisation

The definition of this SFR is present in [PP-eUICC] and it is unchanged within this ST.

6.1.7 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE,**

Tuak, [assignment: *Cave]*[49] and cryptographic key sizes **according to the corresponding standard that meet the following:

- **MILENAGE according to standard [MILENAGE] with the following restrictions:**
    - **Only use 128-bit AES as the kernel function - do not support other choices**
    - **Allow any value for the constant OP**
    - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [MILENAGE]**
- **Tuak according to [Tuak] with the following restrictions:**
    - **Allow any value of TOP**
    - **Allow multiple iterations of Keccak**
    - **Support 256-bit K as well as 128-bit**
    - **To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.**
- **[selection: [assignment: *Cave according to standard [CAVE] with the following restrictions:***
    - ***Supports 0~16 rounds of SSD Generation[50]]]***[51]**.**

FCS_CKM.2/Mobile_network Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[assignment: *Profile download and installation]***[52] that meets the following: **[assignment: *[SGP.22] §3.1.3, §5.7.6 and* [SGP.32] *§3.2, §8.6.3, [SIMalliance], §8.6.3, [SIMalliance_2] §8.6.3]***[53].

FCS_CKM.6/Mobile_network Cryptographic key destruction

[49] [selection:[assignment: cryptographic algorithms], *no other algorithm*]
[50] [assignment: *list of standards*]
[51] [selection: *[assignment: list of standards], no additional standards*]
[52] [assignment: *cryptographic key distribution method*]
[53] [assignment: *list of standards*]

FCS_CKM.6.1/Mobile_network The TSF shall destroy **MILENAGE keys, TUAK keys and [selection: [assignment: *Cave keys*][54]]**[55] when **[selection: *no longer needed*]**[56].

FCS_CKM.6.2/ Mobile_network The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/Mobile_network in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values*]**[57] that meets the following: **[assignment: *none*]**[58].

---

54 [assignment; keys of the cryptographic algorithms]

55 [selection: [assignment; keys of the cryptographic algorithms], no other keys of the cryptographic algorithm]

56 [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]]

57 [assignment: cryptographic key destruction method]

58 [assignment: list of standards]

6.2 Java Card System SFRs

In the Protection Profile [PP-eUICC] the objectives for the Runtime Environment are defined as objectives for the environment (OE.RE.*). Since the IC and the RE is part of the TOE of this ST, the objectives for the environment were translated into objectives for the TOE (as shown in section 4.1). They subsequently have to be covered by SFRs that have been imported here from the Java Card PP [PP-JCS] (as shown in section 2.5.3.9). The following subsections address only those SFRs where assignments and selections were made by the ST author.

This ST includes the Subjects, Objects, Information and Security attributes from the [PP-JCS], Section 7.2, as required by the SFRs.

6.2.1 CoreG_LC Security Functional Requirements

6.2.1.1 Firewall Policy

FDP_IFF.1/JCVM Simple security attributes

FDP_IFF.1.3/JCVM The TSF shall enforce the **[assignment: *following additional information flow control SFP rules: none*]**[59].

FDP_IFF.1.4/JCVM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[60].

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **[assignment: *none*]**[61].

The definition of the following SFRs is present in [PP-JCS] and it is unchanged within this ST:

FDP_ACC.2/FIREWALL Complete access control

[59] [assignment: *additional information flow control SFP rules*]
[60] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[61] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

FDP_ACF.1/FIREWALL Security attribute based access control

FDP_IFC.1/JCVM Subset information flow control

FDP_RIP.1/OBJECTS Subset residual information protection

FMT_MSA.1/JCRE Management of security attributes

FMT_MSA.1/JCVM Management of security attributes

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

FMT_MSA.3/FIREWALL Static attribute initialisation

FMT_MSA.3/JCVM Static attribute initialisation

The definition of the following SFRs is present in [PP-JCS] and it is unchanged within this ST, except the iteration /RE:

FMT_SMF.1/RE Specification of Management Functions

FMT_SMR.1/RE Security roles

6.2.1.2 Application Programming Interface

FCS_CKM.1 Cryptographic key generation

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

Iteration	Cryptographic key generation algorithm	Cryptographic key sizes	List of standards
/ECC	G+D EC key generator	NIST P-256	[RFC5639] chapter 3
/Triple DES	G+D Triple DES key generator	112, 168 bits	[SP800-67] chapters 3.3.1 and 3.3.2
/AES	G+D AES key generator	128, 192 and 256 bits	[FIPS197] chapters 3.1 and 5

FCS_CKM.6/RE replaces FCS_CKM.4 of [PP-JCS].

FCS_CKM.6/RE Timing and event of cryptographic key destruction

FCS_CKM.6.1/RE The TSF shall destroy **[assignment: *ECC keys, Triple DES keys, AES keys*]**[62] when **[selection: *no longer needed*]**[63].

FCS_CKM.6.2/RE The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/RE in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting the keys with zero values*]**[64] that meets the following: **[assignment: *none*]** [65].

FCS_COP.1 Cryptographic operation

[62] [assignment: *list of cryptographic keys (including key material)*]
[63] [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction]*]
[64] [assignment: *cryptographic key destruction method*]
[65] [assignment: *list of standards*]

FCS_COP.1.1 The TSF shall perform **[assignment: *the cryptographic operations in Table 19*]**[66] in accordance with a specified cryptographic algorithm **[assignment: *in Table 19*]**[67] and cryptographic key sizes **[assignment: *in Table 19*]**[68] that meet the following: **[assignment: *list of standards in Table 19*]**[69].

[66] [assignment: *list of cryptographic operations*]
[67] [assignment: *cryptographic algorithm*]
[68] [assignment: *cryptographic key sizes*]
[69] [assignment: *list of standards*]

Iteration	Operation	Algo-rithm	Key sizes	List of standards
/SHA	hashing	SHA-256, 384, 512	n.a.	[FIPS180-4]
/SIG_ECC	digital signa-ture generation and verification	ECDSA	256 bits	[FIPS186-4] [BSI TR 03111] [RFC5639]
/MAC_TDES	MAC genera-tion and verifi-cation	Triple-DES CBC MAC	112, 168 bits	[FIPS46-3], Chapter 'TRIPLE DATA EN-CRYPTION ALGO-RITHM', [ISO 9797-1] Sections 6.6.3, 7.1, 7.3
/MAC_AES		AES CBC MAC, AES CMAC	128, 192, 256 bits	[FIPS197] Section 5 [ISO 9797-1] Section 7.1 [SP800-38b] Section 6
/CIPH_TDES	encryption and decryption	Triple-DES in CBC	112, 168 bits	[SP800-67] [SP800-38a]
/CIPH_AES	encryption and decryption	AES in CBC and ECB modes	128, 192, 256 bits	[FIPS197] [SP800-38a]
/CIPH_AES_GCM	encryption and decryption	AES in GCM mode	128 bits	[FIPS197] [SP800-38d]

/ECKA-EG	Key agreement	ElGamal elliptic curves key agreement	256 bits	NIST P-256 acc. to [FIPS186-4], [BSI TR-03111]

Table 19 List of cryptographic operations

Application note 16:
The cryptographic algorithms stated below of FCS_COP.1 are not provided as a service via JavaCard API.

FCS_COP.1 supports the requirements of [SGP.22] related to cryptographic mechanisms used for:

(1) User authentication (FIA_UAU.1/EXT):

- *A U.SM-DP+ must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.DPauth.ECDSA and CERT.DPpb.ECDSA), as well as the public key of the CI (D.PK.CI.ECDSA). Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography of the TOE is compliant to following:*
    - *NIST P-256, defined in Digital Signature Standard (recommended by NIST);*
    - *brainpoolP256r1, defined in RFC 5639 (recommended by BSI).*

- *U.MNO-OTA must be authenticated using a SCP80 secure channel according to [TS102 225] and [TS102 226] using the parameters defined in [RFC3447] §2.4.3, or optionally SCP81 according to [GP AM B] using the parameters defined in [RFC3447] §2.4.4 (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO).*

(2) Establishment of and secure communication over trusted channels (FTP_ITC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP) by providing the

required cryptographic algorithms for the SCP-SGP22, SCP80 and SCP81.

The TOEs underlying cryptography for the ElGamal elliptic curves key agreement (ECKA) is complaint with NIST P-256 (FIPS PUB 186-3 Digital Signature Standard) only.

The definition of the following SFRs is present in [PP-JCS] and it is unchanged within this ST:

FDP_RIP.1/ABORT Subset residual information protection

FDP_RIP.1/APDU Subset residual information protection

FDP_RIP.1/bArray Subset residual information protection

FDP_RIP.1/GlobalArray Subset residual information protection

FDP_RIP.1/KEYS Subset residual information protection

FDP_RIP.1/TRANSIENT Subset residual information protection

FDP_ROL.1/FIREWALL Basic rollback

6.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take one of the following actions:

- **throw an exception,**
- **lock the card session,**
- **reinitialize the Java Card System and its data**
- **[assignment: *other actions: Card Lock / Application Lock*]**[70]

upon detection of a potential security violation.

Refinement:

The "potential security violation" stands for one of the following events:

- CAP file inconsistency,

[70] [assignment: *list of other actions*]

- typing error in the operands of a bytecode,
- applet life cycle inconsistency,
- card tearing (unexpected removal of the card out of the CAD) and power failure,
- abort of a transaction in an unexpected context (see abortTransaction(), [JCAPI] and [JCRE], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow,
- **[assignment: *flow control errors,***
- ***other runtime errors related to applet's failure (like uncaught exceptions)]***[71].

Application note 17:

Bytecode verification is performed off-card.

FDP_SDI.2/DATA Stored data integrity monitoring and action

FDP_SDI.2.1/DATA The TSF shall monitor user data stored in containers controlled by the TSF for **[assignment: integrity errors]**[72] on all objects, based on the following attributes: **[assignment: *checksum integrity (complementary value, Error Detection Code) of cryptographic keys, PIN values and their associated attributes]***[73].

FDP_SDI.2.2/DATA Upon detection of a data integrity error, the TSF shall **[assignment: *bring the card into a secure state]***[74].

FPR_UNO.1 Unobservability

[71] [assignment: *list of other runtime errors*]
[72] [assignment: integrity errors]
[73] [assignment: *user data attributes*]
[74] [assignment: *actions to be taken*]

FPR_UNO.1.1 The TSF shall ensure that **[assignment: *unauthorized users or subjects*]**[75] are unable to observe the operation **[assignment: *cryptographic operations, comparison operations*]**[76] on **[assignment: *key values, PIN values*]**[77] by **[assignment: *S.JCRE, S.Applet, S.SD, S.OSU, S.UpdateImageCreator*]**[78].

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

FPT_TDC.1.2/RE The TSF shall use

- **the rules defined in [JCVM] specification,**
- **the API tokens defined in the export files of reference implementation**,
- **[assignment: *no other rules*]**[79]

when interpreting the TSF data from another trusted IT product.

The definition of the following SFR is present in [PP-JCS] and it is unchanged within this ST, except the iteration /RE:

FPT_FLS.1/RE Failure with preservation of secure state

6.2.1.4 AID Management

FIA_USB.1/AID User-subject binding

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: *rules defined in FMT_MSA.2/FIREWALL_JCVM and FMT_MSA.3.1/FIREWALL*]**[80].

FIA_USB.1.3/AID The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the

[75] [assignment: *list of users and/or subjects*]
[76] [assignment: *list of operations*]
[77] [assignment: *list of objects*]
[78] [assignment: *list of protected users and/or subjects*]
[79] [assignment: *list of interpretation rules to be applied by the TSF*]
[80] [assignment: *list of rules for the initial association of attributes*]

behalf of users: **[assignment: *rules defined in FMT_MSA.3.1/FIREWALL]***[81].

The definition of the following SFRs is present in [PP-JCS] and it is unchanged within this ST:

FIA_ATD.1/AID User attribute definition

FIA_UID.2/AID User identification before any action

FMT_MTD.1/JCRE Management of TSF data

FMT_MTD.3/JCRE Secure TSF data

6.2.2 InstG Security Functional Requirements

The InstG SFRs are not included. They are replaced by the following SFRs from [PP GP] as defined in section 6.3:

FDP_ITC.2/GP-ELF replaces FDP_ITC.2/Installer of [PP-JCS].

FMT_SMR.1/GP replaces FMT_SMR.1/Installer of [PP-JCS].

FPT_FLS.1/GP replaces FPT_FLS.1/Installer of [PP-JCS].

FPT_RCV.3/GP replaces FPT_RCV.3/Installer of [PP-JCS].

6.2.3 ADELG Security Functional Requirements

All SFRs of this group are included from [PP-JCS] without modification:

FDP_ACC.2/ADEL Complete access control

FDP_ACF.1/ADEL Security attribute based access control

FDP_RIP.1/ADEL Subset residual information protection

FMT_MSA.1/ADEL Management of security attributes

FMT_MSA.3/ADEL Static attribute initialisation

[81] [assignment: *list of rules for the changing of attributes*]

FMT_SMF.1/ADEL Specification of Management Functions

FMT_SMR.1/ADEL Security roles

FPT_FLS.1/ADEL Failure with preservation of secure state

6.2.4 ODELG Security Functional Requirements

All SFRs of this group are included from [PP-JCS] without modification:

FDP_RIP.1/ODEL Subset residual information protection

FPT_FLS.1/ODEL Failure with preservation of secure state

6.2.5 CarG Security Functional Requirements

The CarG SFRs are not included. They are replaced by the following SFRs from [PP GP] as defined in section 6.3:

FCO_NRO.2/GP replaces FCO_NRO.2/CM of [PP-JCS].

FDP_IFC.2/GP-ELF replaces FDP_IFC.2/CM of [PP-JCS].

FDP_IFF.1/GP-ELF replaces FDP_IFF.1/CM of [PP-JCS].

FDP_UIT.1/GP replaces FDP_UIT.1/CM of [PP-JCS].

FIA_UID.1/GP replaces FIA_UID.1/CM of [PP-JCS].

FMT_MSA.1/GP replaces FMT_MSA.1/CM of [PP-JCS].

FMT_MSA.3/GP replaces FMT_MSA.3/CM of [PP-JCS].

FMT_SMF.1/GP replaces FMT_SMF.1/CM of [PP-JCS].

FTP_ITC.1/GP replaces FTP_ITC.1/CM of [PP-JCS].

6.3 Card Content Management SFRs

The Runtime Environment shall provide secure means for card management activities ([PP-eUICC], section 4.2.2, OE.RE.PRE-PPI). Since the Runtime Environment is part of the TOE of this ST, the corresponding objectives were transformed into objectives for the TOE (O.RE.PRE-PPI) and subsequently have to be covered by SFRs. Therefore the following SFRs are introduced.

These SFRs replace the SFRs from the [PP-JCS] as stated in sections 6.2.2 and 6.2.5.

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **[selection: [assignment: *1*][82]]** [83] 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.**

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: *receive*]**[84] 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.

---

[82] [assignment: positive integer number]
[83] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[84] [selection: transmit, receive]

Application note 18:

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

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

FDP_ROL.1/GP Basic rollback

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

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

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

FDP_UCT.1/GP Basic data exchange confidentiality

FDP_UCT.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to [**selection: *receive***][85] user data in a manner protected from unauthorised disclosure.

[85] [selection: transmit, receive]

Application note 19:

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.

FDP_IFC.2/GP-ELF Complete information flow control

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

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

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

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

Application note 20:

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 [GP] Chapter 11 and Appendix A.1, respectively.

FDP_IFC.2/GP-KL Complete information flow control

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

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

- **Information: GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys** and all operations that cause that information to flow to and from subjects covered by the SFP.

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

Application note 21:

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

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

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 from FMT_MSA.1/GP SFR*]**[86] to specify alternative initial values to override the default values when an object or information is created.

Application note 22:

This SFR refines FMT_MSA.3/CM of [PP-JC]. It is extended to cover the Data and Key loading Policy.

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

[86] [assignment: authorised identified roles]

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: *[assignment: perform the operations listed in the tables below]*]**[87] the security attributes **[assignment: *listed in the tables below*]**[88] to **[assignment: *the authorised identified roles listed in the tables below*]**[89].

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

87 [selection: change_default, query, modify, delete, [assignment: other operations]]
88 [assignment: list of security attributes]
89 [assignment: the authorised identified roles]

SET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, CARD_LOCKED, or TERMINATED	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD

Table 20 GlobalPlatform Common Operations, Security Attributes, and Roles

<table>
<tr><th>Operations:

SCP02 Commands</th><th>Security Attributes:

Card Life Cycle State</th><th>Security Attributes:

Minimum Security Level</th><th>Authorised Identified

Roles with Privileges</th></tr>
<tr><td>INITIALIZE UPDATE</td><td rowspan="2">OP_READY, INITIALIZED, SECURED, or CARD_LOCKED</td><td>None</td><td rowspan="2">ISD, AM SD, DM SD, SD</td></tr>
<tr><td>EXTERNAL AUTHENTICATE</td><td>C-MAC</td></tr>
</table>

Table 21 SCP02 Operations, Security Attributes, and Roles

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

Table 22 SCP11 Operations, Security Attributes, and Roles

Operations: SCP80 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
Remote File Management Commands SELECT UPDATE BINARY UPDATE RECORD SEARCH RECORD INCREASE VERIFY PIN CHANGE PIN DISABLE PIN ENABLE PIN UNBLOCK PIN DEACTIVATE FILE	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]

ACTIVATE FILE READ BINARY READ RECORD CREATE FILE DELETE FILE RESIZE FILE SET DATA RETRIEVE DATA			
Remote Applet Management Commands DELETE SET STATUS INSTALL LOAD PUT KEY GET STATUS GET DATA STORE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]

Table 23 SCP80 Operations, Security Attributes, and Roles

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

Table 24 SCP81 Operations, Security Attributes, and Roles

Legend:

ISD: Issuer Security Domain

AM SD: Security Domain with Authorised Management privilege

DM SD: Security Domain with Delegated Management privilege

SD: Other Security Domain

Application note 23:

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 24:

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).

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

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

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

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

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

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

- **The algorithms and key sizes of the imported keys shall be supported by the SE**
- **[assignment: *none*][90].**

Application note 25:

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

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

FTP_ITC.1/GP Inter-TSF trusted channel

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

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

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

- **APDU commands sent to the card within a Secure Channel Session**
- **When loading/installing a new ELF on the card**
- **When transmitting and loading sensitive data to the card using STORE DATA or PUT KEY commands**

[90] [assignment: additional importation control rules]

- **When deleting ELFs, Applications, or Keys**
- **[assignment:**
    - ***When retrieving status information via GET STATUS Command***
    - ***When modifying the Application Life Cycle State via SET STATUS command*]**[91]**.**

Application note 26:

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: *Executable Load Files, SD/Application data and keys*]**[92] 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: *identity*]**[93] of the originator of the information, and the **[assignment: Executable Load Files, SD/Application data and keys]**[94] of the information to which the evidence applies.

Refinement

---

[91] [assignment: *list of functions for which a trusted channel is required*]
[92] [assignment: *list of information types*]
[93] [assignment: *list of attributes*]
[94] [assignment: *list of information fields*]

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: *that the data origin authentication provided within the context of secure messaging was successful*]**[95].

Application note 27:

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.

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:**

- ***Subjects: S.SD, S.OPEN***
- ***Information: INSTALL and LOAD commands***
- ***Security Attributes: card Life Cycle State, SD Life Cycle states, Secure Channel Security Level, SD privileges]***[96].

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:

[95] [assignment: *limitations on the evidence of origin*]
[96] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

- **S. SD implements one or more Secure Channel Protocols, namely [selection: *SCP02, SCP03, SCP11, SCP80, SCP81*][97], each with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **On receipt of INSTALL or LOAD commands, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **S.OPEN accepts an ELF only if its integrity and authenticity has been verified.**
- **[assignment: *S.OPEN accepts an ELF only if its AID is not already registered by the TSF*][98].**

FDP_IFF.1.3/GP-ELF The TSF shall enforce the **[assignment: *none*]**[99].

FDP_IFF.1.4/GP-ELF The TSF shall explicitly authorise an information flow based on the following rules**: [assignment: *none*]**[100].

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

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- **S.OPEN fails to verify the Card Life Cycle state**
- **S.OPEN fails to verify the SD privileges.**
- **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.SD fails to unwrap INSTALL or LOAD commands.**

---

[97] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]
[98] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]
[99] [assignment: additional information flow control SFP rules]
[100] [assignment: rules, based on security attributes, that explicitly authorise information flows]

- **[assignment: *none*]**[101]**.**

Application note 28

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

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

• For INSTALL, see [GP] section 11.5.

• For LOAD, see [GP] section 11.6.

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

The minimum security level of INSTALL and LOAD is 'AUTHENTICATED' as defined in [GP] section 10.6.

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

For more details about the rules to be applied to each role of INSTALL command, refer to [GP] 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.

[101] [assignment: rules, based on security attributes, that explicitly deny information flows]

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

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

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

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

- **Referring to Java Card rules defined in [JCVM] and [JCRE]: ELF loading is allowed only if, for each dependent ELF, its AID attribute is equal to a resident ELF AID attribute, and the major (minor) Version attribute associated with the dependent ELF is less than or equal to the major (minor) Version attribute associated with the resident ELF**
- **[assignment: *none*]**[102]**.**

Application note 29

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

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

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

FDP_IFF.1/GP-KL Complete information flow control

[102] [assignment: additional importation control rules]

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:**

- ***Subjects: S.SD, S.OPEN***
- ***Information: STORE DATA and PUT KEY commands***
- ***Security Attributes: card Life Cycle State, SD Life Cycle states, Secure Channel Security Level*]**[103].

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection: *SCP02, SCP03, SCP11, SCP80, SCP81*][104], each equipped with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application,**
- **S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the**
- **S.OPEN checks that the requesting S.SD has no restrictions for personalisation.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and prior to the command forwarding to the targeted Application or SD.**

---

[103] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]
[104] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]

- **[assignment: *none*][105].**

FDP_IFF.1.3/GP-KL The TSF shall enforce the **[assignment: *none*][106].**

FDP_IFF.1.4/GP-KL The TSF shall explicitly authorise an information flow based on the following rules**: [assignment: *none*][107].**

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

- **S.OPEN fails to verify the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to unwrap STORE DATA or PUT KEY.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **[assignment: *none*][108].**

Application note 30

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

- For PUT KEY, see [GP] section 11.8.

- For STORE DATA, see [GP] section 11.11.

[105] [assignment: for each operation, the security attribute-based re-lationship that must hold between subject and information secu-rity attributes]
[106] [assignment: additional information flow control SFP rules]
[107] [assignment: rules, based on security attributes, that explicitly author-ise information flows]
[108] [assignment: rules, based on security attributes, that explicitly deny information flows]

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

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

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

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

FMT_SMF.1/GP Specification of Management Functions

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

- **Card and Application Security Management as defined in [GP] : 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 [GP].**

Application note 31:

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 [GP] Chapter 10.

Card Termination is not supported by the TOE.

FPT_RCV.3/GP Automated recovery without undue loss

FPT_RCV.3.1/GP When automated recovery from **[assignment: *power loss*]**[109] 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: *a failure during load/installation of a package/applet and deletion of a package/applet/object*]**[110] 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: *0%*]**[111] 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 32

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

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

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

Examples of failures include interruption of the installation of an Executable Load File, interruption of a package/application deletion, loss of the integrity

[109] [assignment: list of failures/service discontinuities during card content management operations]
[110] [assignment: list of failures/service discontinuities during card content management operations]
[111] [assignment: quantification]

of Executable Load File, and error during linking of an executable Load File with the Files already present in the card. The behaviour of the TSF is implementation-dependent.

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

FPT_FLS.1/GP Failure with preservation of secure state

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

- **S.OPEN fails to load/install an Executable Load File / Application instance.**
- **S.SD fails to load SD/Application data and keys.**
- **S.OPEN fails to verify/change the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **[assignment: *none*][112].**

Application note 33

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

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

112 [assignment: list of additional types of fail-ures]

FIA_UID.1/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **[assignment: *SD selection, application selection, Initializing a Secure Channel with the card, requesting data that identifies the card or off-card entities*]**[113] 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 34:

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.

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: *none*]**[114] 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: *none*]**[115] when interpreting the TSF data from another trusted IT product.

Application note 35:

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 [GP] sections 11.5, 11.6, 11.8, and 11.11.

---

[113] [assignment: list of TSF-mediated actions]
[114] [assignment: list of TSF data types]
[115] [assignment: list of interpretation rules to be applied by the TSF]

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**.

6.4 Secure IC Platform SFRs

The IC embedded software does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code against disclosure or modification ([PP-eUICC], section 4.2.2, OE.IC.SUPPORT (1)). Since the IC platform is part of the TOE of this ST, the related objectives for the environment were redefined as objectives for the TOE (O.IC.SUPPORT); they subsequently have to be covered by SFRs.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **[assignment: *physical manipulation and physical probing*]**[116] to the **[assignment: *TSF*]**[117] by responding automatically such that the SFRs are always enforced.

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **[assignment: *the process before TOE Delivery*]**[118] with the capability to store **[selection: *Initialisation Data*]**[119] in the **[assignment: *NVM*]**[120].

Application note 36

Initialisation Data is data that is loaded by the Initialiser during eUICC lifecycle phase b.

[116] [assignment: *physical tampering scenarios*]
[117] [assignment: *list of TSF devices/elements*]
[118] [assignment: *list of subjects*]
[119] [selection: *the Initialisation Data, Pre-personalisation Data, [assignment: other data]*]
[120] [assignment: *type of persistent memory*]

FPT_RCV.3/OS Automated recovery without undue loss

FPT_RCV.3.1/OS When automated recovery from **[assignment: *none*]**[121], 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/OS For **[assignment: *execution access to a memory zone reserved for TSF data, writing access to a memory zone reserved for TSF's code, and any segmentation fault performed by a Java Card applet*]**[122] the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/OS 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:

- ***the contents of Java Card static fields, instance fields, and array positions that fall under the scope of an open transaction;***
- ***the Java Card objects that were allocated into the scope of an open transaction;***
- ***the contents of Java Card transient objects;***
- ***any possible Executable Load File being loaded when the failure occurred*]**[123]

for loss of TSF data or objects under the control of the TSF.

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

Application note 37

There is no maintenance mode implemented within the TOE. Recovery is always enforced automatically as stated in FPT_RCV.3.2/OS.

[121] [assignment: *list of failures/service discontinuities*]
[122] [assignment: *list of failures/service discontinuities*]
[123] [assignment: *quantification*]

FPT_RCV.4/OS Function Recovery

FPT_RCV.4.1/OS The TSF shall ensure that [assignment: *reading from and writing to static and objects' fields interrupted by power loss*][124] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

[124] [assignment: list of functions and failure scenarios]

6.5 OS Update (ITL) SFRs

The following SFR are related to the eUICC OS Update capability.

6.5.1 Class FDP: User Data Protection

FDP_ACC.1/OS-UPDATE Subset access control

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

- **Subjects: S.OS-DEVELOPER is the representative of the OS Developer within the TOE, being responsible for signature verification and decryption of the additional code, before:**
  - **Loading**
  - **Installation**
  - **Activation**
  - **[assignment: *Eligibility*]**[125]

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

Application note 38

It is applied the following correspondence in [PP-GP] and [PP-eUICC]:

S.OS-DEVELOPER corresponds to S.OSU.

Eligibility is a validation that the additional OS will be compatible before accepting its download. This is the initial operation and it ensures the compatibility of the additional OS, and performs authentication verification, decryption and integrity assurance.

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

[125] [assignment: list of other subjects covered by the SFP]

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: *The integrity check of the manifest, received package, and written memory ensures that the OS Update operation is successful.*].**[126]

FDP_ACF.1.3/OS-UPDATE The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *none*]**[127]**.**

FDP_ACF.1.4/OS-UPDATE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: *none*]**[128]**.**

---

126 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
127 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
128 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

Application note 39

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 Confidentiality protection is achieved through direct encryption of the additional code.

Additionally, it is applied the following correspondence in [PP-GP] and [PP-eUICC]:

S.OS-DEVELOPER	*S.OSU*
D.OS-UPDATE_DEC-KEY D.OS-UPDATE_SGNVER-KEY	*D.OS-UPDATE_KEY(S)*
OE.CONFID_UPDATE_IMAGE.CREATE	*OE.OS-UPDATE-ENCRYPTION*

6.5.1 Class FMT: Security Management

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 40

The additional code signature verification status must be set to “Fail” by default. This prevents installation of any additional code until the additional code signature is successfully verified by the TOE.

FMT_SMR.1/OS-UPDATE Security roles

FMT_SMR.1.1/OS-UPDATE The TSF shall maintain the roles **OS Developer, Issuer**.

FMT_SMR.1.2/OS-UPDATE The TSF shall be able to associate users with roles.

FMT_SMF.1/OS-UPDATE Specification of Management Functions

FMT_SMF.1.1/OS-UPDATE The TSF shall be capable of performing the following management functions: **activation of additional code**.

Application note 41

Additional code means entire OS.

Once verified and installed, additional code needs to be activated to become effective.

6.5.2 Class FIA: Identification and Authentication

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.

6.5.3 Class FTP: Trusted Path/Channels

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: *none*]**[129].

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 42

During the transmission of the additional code to the TOE for loading, the confidentiality is ensured through direct encryption of the additional code. Consequently, it is selected 'none' in FTP_TRP.1.1/OS-UPDATE.

6.5.4 Class FCS: Cryptographic support

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: *AES in GCM mode*]**[130] and cryptographic key sizes **[assignment: *128 bits*]**[131] that meet the following: **[assignment: *[FIPS197], [SP800-38d]*]**[132].

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

[129] [selection: disclosure, none]
[130] [assignment: cryptographic algorithm]
[131] [assignment: cryptographic key sizes]
[132] [assignment: list of standards]

specified cryptographic algorithm **[assignment: *AES CMAC*]**[133]and crypto-graphic key sizes **[assignment: *128 bits*]**[134] that meet the following: **[assignment: *[FIPS197], [SP800-38b]*]**[135].

6.5.5 Class FPT: Protection of the TSF

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 43

The OS Update operation must either be successful or fail securely.

There are 5 steps in an OS Update operation:

- *Step 1: eligibility check*
- *Step 2: loading*
- *Step 3: activation*
- *Step 4: update of TOE identification data*

Step 1 is a blocker, so that if the new OS is not compatible with the current TOE, the update will not proceed and no changes will be applied on the TOE.

Steps 2 to 4 are performed subsequently, being step 4 only accepted in case all the previous steps have been fulfilled.

- *If a failure (interruption or incident) occurs during step 1 (eligibility), then the TOE remains in its initial state (no update, neither of code nor of the TOE identification data).*

133 [assignment: cryptographic algorithm]
134 [assignment: cryptographic key sizes]
135 [assignment: list of standards]

- *If a failure (interruption or incident) occurs during step 2, the TOE will remain in a safe state, being the ITL in charge of the TOE, and waiting for the failed update to be started from scratch. Only the same OS that was interrupted is eligible, other OS update attempts will be rejected.*
- *Steps 3 and 4 are performed in an atomic way. If a failure (interruption or incident) occurs in these steps, the activation will be restarted, followed by the update of TOE identification data, after performing a RESET of the card.*

6.6 Security Requirements Dependencies

The Security Functional Requirements dependencies for the eUICC component are the same as in the eUICC Base-PP [PP-eUICC], section 6.3.3.1.

The Security Functional Requirements dependencies for the RE are the same as in the Java Card PP [PP-JCS].

The dependency to FCS_COP.1/SIG_ECC for the public key of the CI (D.PK.CI.ECDSA) is left unsatisfied since it is loaded pre-issuance of the TOE.

The SFRs Dependencies tables are extended by the following the following table. The SARs Dependencies tables are not extended.

Security Functional Requirement	**Dependencies**	**Satisfied Dependencies**
FCS_COP.1/SIG_ECC In case the public key included in its certificates CERT.DPauth.ECDSA and CERT.DPpb.ECDSA is based on brainpoolP256r1.	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FDP_ITC.2/SCP FCS_CKM.6
FCS_COP.1/SIG_ECC In case the key is based on NIST P-256 curve.	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FCS_CKM.1 FCS_CKM.6
FCS_PHP.3	No Dependencies	No Dependencies

Table 25 Extension of SFR Dependencies

The Security Functional Requirements dependencies for the Card Content Management are from [PP-GP], section 7.3.3.1, as follows:

Security Functional Requirement	**Dependencies**	**Satisfied Dependencies**
FIA_AFL.1/GP	FIA_UAU.1 Timing of authentication	FIA_UAU.1/GP
FIA_UAU.1/GP	FIA_UID.1 Timing of identification	FIA_UID.1/GP
FIA_UAU.4/GP	No Dependencies	No Dependencies
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
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
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_IFC.2/GP-KL	FDP_IFF.1 Simple security attributes	FDP_IFF.1/GP-KL

FDP_IFC.2/GP-ELF	FDP_IFF.1 Simple security attributes	FDP_IFF.1/GP-ELF
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_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_SMR.1/GP	FIA_UID.1 Timing of identification	FIA_UID.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_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
FTP_ITC.1/GP	No Dependencies	No Dependencies
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_SMF.1/GP	No Dependencies	No Dependencies
FIA_UID.1/GP	No Dependencies	No Dependencies
FPT_TDC.1/GP	No Dependencies	No Dependencies
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_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

The Security Functional Requirements dependencies for the OS update (ITL) module are from the GlobalPlatform PP-Module OS update [PP-GP] as follows:

Security Functional Requirement	**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
FMT_MSA.3/OS-UPDATE	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_SMR.1/OS-UPDATE See rationale.
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, or FCS_CKM.5 Cryptographic key derivation)	FDP_ITC.2/GP-ELF FCS_CKM.6/RE

	FCS_CKM.6 Cryptographic key destruction	
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, or FCS_CKM.5 Cryptographic key derivation) FCS_CKM.6 Cryptographic key destruction	FDP_ITC.2/GP-ELF FCS_CKM.6/RE

Table 26 OS Update SFR Dependencies

The dependency FMT_MSA.1 of FMT_MSA.3/OS-UPDATE is discarded as no history information has to be kept by the TOE.

6.7 Security Functional Requirements Rationale

6.7.1 SFRs for eUICC rationale

The security functional requirements rationale is the same to the one present in section 6.3 in [PP-eUICC].

6.7.2 SFRs for Runtime Environment rationale

The security functional requirements rationale of [PP-JCS] Section 7.4 applies.

For the translated objectives of the underlying IC platform and the Runtime Environment, the rationale from the Java Card System SFRs that are covered by the security objectives related to the threats defined in [PP-JCS] applies.

The next table shows the objectives related to [PP-eUICC] runtime environment and its translation according to [PP-eUICC] application notes for OE.RE* objectives. The security functional requirements rationale of O.RE* will be the same as the rationale for the objectives translated from Java Card PP [PP-JCS] and are not repeated here.

In case of O.CARD-MANAGEMENT, the Security Functional Requirements rationale are extracted from [PP-GP].

In case of Objectives for the OS Update, the SFRs rationale is extracted from [PP-GP].

RE objectives	**Translation from Java Card PP**
O.RE.PRE-PPI	O.INSTALL, O.DELETION, O.LOAD, O.CARD-MANAGEMENT
O.RE.SECURE-COMM	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.ALARM,

	O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION
O.RE.API	O.CARD-MANAGEMENT, O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM
O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT
O.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE

OE.SCP.RECOVERY and OE.SCP.SUPPORT from [PP-JCS] are equivalent to OE.IC.RECOVERY and OE.IC.SUPPORT from [PP-eUICC] converted to O.IC.RECOVERY and O.IC.SUPPORT in current Security Target. See next section for the rationale.

6.7.3 SFRs for Underlying platform IC rationale

Objective	**SFRs**	**Rationale / statement on contribution to the objective coverage**
O.IC.SUPPORT	FCS_CKM.1/*, FCS_CKM.6/*, FAU_ARP.1, FPR_UNO.1, FPT_EMS.1/Base, FPT_PHP.3, FDP_SDI.2/DATA, FDP_ROL.1/FIREWALL FPT_RCV.4/OS	Contribute by resetting the card session or terminating the card in case of physical tampering; by ensuring leakage resistant implementations of the unobservable operations; by preventing bypassing, deactivation or changing of other security features. Contribute to resistance against physical attacks, to non-bypassability by securing data against modification, and to low-level-cryptographic support and low-level transaction mechanism.
O.IC.RECOVERY	FAU_ARP.1, FPT_FLS.1/RE FPT_RCV.3/OS	Contribute by ensuring reinitialization of the Java Card System and its data after card tearing and power failure, and by preserving a secure state after failure.
O.IC.PROOF_OF_IDENTITY	FAU_SAS.1	Contributes to providing the off-card actor with a cryptographic proof of identity based on an EID, which is derived form eUICC hardware identification.

Table 27 IC Security Objectives and SFRs – Coverage

6.7.4 SFR for Card Content Management rationale

Objective	SFR and Rationale / statement on contribution to the objective coverage (extracted from [PP-GP] section 7.3.1.2)
O.CARD-MANAGE-MENT	FDP_UIT.1/GP ensures the integrity of card management operations. FDP_UCT.1/GP ensures the confidentiality of card management operations. FDP_ROL.1/GP ensures the rollback of the installation or removal operation on the executable files and application instances. FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs. FDP_ITC.2/GP-KL enforces the Data & Key information flow policy when importing keys and data. FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting an Executable File / application instance. FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the information flow control policy for managing, authenticating, and protecting the Card management commands and responses between off-card and on-card entities. FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, these SFRs specify the actions being performed before the authentication of the origin of the received APDU commands takes place. FCO_NRO.2/GP enforces the evidence of the origin during the loading of Executable Load Files, SD/Application data and keys. FPT_TDC.1/GP specifies requirements preventing any possible misinterpretation of the Security Domain keys used to implement a Secure Channel when those are loaded from the off-card entity.

	FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data. FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to: o ensure the authenticity, integrity, and/or confidentiality of card management commands; o enforce the TOE Life cycle management and transitions. FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands. FMT_SMR.1/GP maintains the roles S.OPEN, ISD, SSD, Application, and their associated Life Cycle states. In addition, it maintains the Application Provider, Controlling Authority roles and specifies the authorised roles enabled for sending and authenticating card management commands. These commands have to be protected with regard to integrity, authenticity, and confidentiality. FPT_RCV.3/GP ensures safe recovery from failure. FIA_AFL.1/GP supports the objective by bounding the number of signatures that the attacker may try to attach to a message to authenticate its origin.

6.7.5 SFRs for OS Update (ITL) rationale

Objective	**Rationale/Statement on contribution to the objective coverage (extracted from [PP-GP], section 18.5)**
O.SECURE_LOAD_ACODE	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the eligibility, loading, installation, and activation of additional code.

	FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code. FCS_COP.1/OS-UPDATE-VER specifies the cryptographic algorithms used to perform digital signature verification of the additional code to be loaded.
O.SECURE_AC_ACTIVATION	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the eligibility, loading, installation, and activation of additional code. FIA_ATD.1/OS-UPDATE maintains the additional code ID for each activated additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code.

	FPT_FLS.1/OS-UPDATE preserves a secure state when upon interruption or incident, which prevents the forming of the Updated TOE.
O.TOE_IDENTIFICATION	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the eligibility, loading, installation, and activation of additional code. FIA_ATD.1/OS-UPDATE maintains the additional code ID for each activated additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code.
O.CONFID-UPDATE-IMAGE.LOAD	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the eligibility, loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation.

	FMT_SMF.1/OS-UPDATE manages the activation of additional code. FTP_TRP.1/OS-UPDATE provides a trusted path during the transmission of the additional code to the TOE for loading. FCS_COP.1/OS-UPDATE-DEC specifies the cryptographic algorithms used to decrypt the additional code prior to installation.
O.AUTH-LOAD-UPDATE-IMAGE	FDP_ACC.1.1/OS-UPDATE enforces the OS Update Access Control Policy on the eligibility, loading, installation, and activation of additional code.

Table 28 OS Update (ITL) Security Objectives and SFRs - Coverage

7. TOE Summary Specification (ASE_TSS)

The Security Functions (SF) introduced in this section realize the SFRs of the TOE.

7.1 SF.TRANSACTION

This security function provides atomic transactions according to the Java Card Transaction and Atomicity mechanism with commit and rollback capability for updating persistent objects in flash memory. The update operation either successfully completes or the data is restored to its original pre-transaction state if the transaction does not complete normally. The transaction exception is thrown if the commit capacity is exceeded during a transaction. The rollback operation restores the original values of the persistent objects and clears the dedicated transaction area.

7.2 SF.ACCESS_CONTROL

This TSF is responsible for enforcing the following security policies:

- ISD-R access control SFP
- ISD-P content access control SFP
- ECASD access control SFP
- FIREWALL access control SFP
- ADEL access control SFP
- JCVM information flow policy
- ELF Loading information flow control SFP (covers INSTALL and LOAD commands)
- Data & Key Loading information flow control SFP (covers STORE DATA and PUT KEY commands)
- Platform services information flow control SFP
- OS Update Access Control Policy

to control the flow of information between subjects and to control the access to objects by subjects.

The TOE provides security management measures:

- Management of security attributes such as Platform data (FMT_MSA.1/PLATFORM_DATA), (FMT_MSA.1/RAT) and keys (FMT_MSA.1/CERT_KEYS) with restrictive default values (FMT_MSA.3);
- Management of roles and security functions (FMT_SMR.1 and FMT_SMF.1).

The TOE enforces access control to objects based on security attributes and throws a security exception when access is denied.

Besides the roles defined in [PP-eUICC] and [PP-JCS], the TOE maintains the roles S.OSU and S.UpdateImageCreator (for OS updates) and S.SD and S.OPEN (for Content Management) and associates users with these roles.

The TOE requires each user to identify itself before allowing TSF-mediated actions on behalf of that user. The TSF associates user security attributes with subjects acting on behalf of that user. The TSF accepts only secure values for security attributes. The TSF provides means to identify remote and on-card users of the TOE.

The TOE requires each user to be successfully authenticated before allowing TSF-mediated actions on behalf of that user. Cryptographic mechanisms used for the authentication are covered by SF.CRYPTO. The TSF prevents prevent reuse of authentication data.

Application selection, secure channel initiation, request data with the GET DATA command on behalf of the user can be performed before the user is identified and authenticated.

The TSF enforces the rules under which

- the S.ISD-R can perform its functions (ISD-R access control SFP in FDP_ACC.1/ISDR and FDP_ACF.1/ISDR),

- the S.ISD-R can perform ECASD functions and obtain output data from these functions (ECASD access control SFP in FDP_ACC.1/ECASD and FDP_ACF.1/ECASD).

The TSF ensures that unauthorized actors shall not get access to or change cryptographic keys. Modification of Security Domain keyset is restricted to its corresponding owner.

In the same manner, the TSF ensures that only the legitimate users can access or change its confidential or integrity-sensitive data.

This domain separation capability relies upon the Runtime Environment protection of applications implemented by the FIREWALL access control SFP and the JCVM information flow policy.

The TOE Runtime Environment capabilities prevent unauthorized code execution by applications and to ensure that native code can be invoked via an API only.

The TOE provides Inter-TSF data consistency and implements rules stated in FPT_TDC.1.2/RE, FPT_TDC.1.2/SCP and FPT_TDC.1/GP when interpreting the TSF data from another trusted IT product.

7.3 SF.INTEGRITY

This TSF provides protection from integrity errors.

The TSF initializes the checksum of cryptographic keys, PIN values and their associated security attributes and monitors cryptographic keys, PIN values and their associated security attributes stored within the TSF for integrity errors by secure verification of the checksum.

Upon detection of a data integrity error the TOE will throw an exception and/or switch to an endless loop and therefore prevent the usage of this key or PIN. This is a secure state.

7.4 SF.SECURITY

This security function provides User data and TSF self-protection measures:

- TOE emanation
- Residual data protection
- Preservation of secure state
- resistance to side channel attacks
- detection of physical tampering

This TSF provides resistance to side channel attacks. The TSF enforces protection of secret data of the TOE during cryptographic operations, comparison operations and key generation against state-of-the-art attacks that are based on external observable physical phenomena of the TOE. The TOE hides information about IC power consumptions and command execution time such that no confidential information can be derived from this data.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource

- deletion of applet instances and/or CAP files,
- in case of failures of PPE, PPI or Telecom Framework,
- from any reference to an object instance created during an aborted transaction,
- sensitive temporary buffers (transient object, bArray object, APDU buffer, Cryptographic buffer) are securely cleared after their usage with respect to their life-cycle and interface as defined in [JCRE],
- transient objects and persistent objects are made inaccessible upon deallocation of the object
- objects owned by the context of an applet instance which triggered the method javacard.framework.JCSystem.requestObjectDeletion().

The card is muted upon detection of a potential security violation such that the TOE preserves a secure state.

The TOE preserves a secure state

- when platform or content management operations fail, e.g.
    - failure of creation of a new ISD-P by ISD-R,
    - failure of installation of a profile by ISD-R,
    - the installer fails to load/install a CAP file/applet,

  - the applet deletion manager fails to delete a CAP file/applet,
  - the object deletion functions fail to delete all the unreferenced objects owned by the applet that requested the execution of the method.
- upon failures that lead to a potential security violation during the processing of a S.PRE, S.PPI or S.TELECOM API specific functions,
- upon failures detected during post-issuance update process (ITL),
- upon detection of a potential security violation described in FAU_ARP.1.

The TOE detects physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. It is resistant to physical tampering of the TSF. If the TOE detects with the above mentioned sensors that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

7.5 SF.PLATFORM_MANAGEMENT

This TSF is responsible for enforcing the Platform services information flow control SFP applicable to the Profile Policy Enabler, Profile Package Interpreter and the Telecom Framework. In particular it defines the measures taken to control the flow of information between the Security Domains and PPE, PPI or Telecom Framework (FDP_IFC.1/Platform_services and FDP_IFF.1/Platform_services).

The TOE provides functionalities of platform management (loading, installation, enabling, disabling, and deletion of applications) in charge of the life-cycle of the whole eUICC and installed applications, as well as the corresponding authorization control, provided by the Profile Policy Enabler (PPE) and the Profile Package Interpreter (PPI).

This functionality relies on the Runtime Environment secure card content management services for loading and installation of a package file, extradition of a package file or an application, personalization of an application or a

Security Domain, deletion of a package file or an application, privileges update of an application or a Security Domain.

Content changes are permitted according to the privileges that have been assigned to the acting Security Domain that holds cryptographic keys used to support the Secure Channel Protocol operations and/or to authorize platform management functions. Before performing platform or content management operations, the TOE checks if the off-card entity has been successfully authenticated and a Secure Channel Session has been successfully initiated. Secure communication is provided by SF.SECURE_CHANNEL.

This TSF relies on the Runtime Environment to ensure the secure identification of the applications it executes.

7.6 SF.SECURE_CHANNEL

This TSF is related to the protection of:

- Profiles downloaded from SM-DP+,
- Commands received from SM-DP+, eIM (SGP.32) and MNO OTA Platform,
- PPR received from the MNO OTA Platform,
- ELF Loading and Data & Key Loading,
- Post-issuance OS Update image loading

by enforcing the following security policies:

- Secure Channel Protocol information flow control SFP,
- ELF Loading information flow control SFP and Data & Key Loading information flow control SFP
- OS Update Access Control Policy

that permit an off-card entity to initiate communication with the TOE via the trusted channel.

Trusted channels provide protection from unauthorized disclosure, modification and replay. Thus the TSF ensures that incoming messages are transmitted are properly provided unaltered to the corresponding Security Domain and that response messages are properly returned to the off-card entity.

The off-card entity may initiate secure communication with the TOE by the following means: SCP02, SCP03, SCP11, SCP-SGP22, SCP80, SCP81.

Secure channel protocol	Algorithms involved
SCP02 (deprecated)	Triple-DES CBC and Triple-DES CBC MAC acc. to [GP] B.1.2.2 (Single DES plus final Triple-DES MAC). Deprecated.
SCP03	AES CBC MAC, AES CMAC [GP AM D]
SCP11	ECDSA 256 bits, AES-128
SCP-SGP22	ECDSA 256 bits, AES-128
SCP80	Triple-DES and AES CBC MAC
SCP81	TLS 1.2 with recommended cipher suites: TLS_PSK_WITH_AES_128_CBC_SHA256 TLS_PSK_WITH_NULL_SHA256 TLS 1.3 with recommended cipher suites: TLS_AES_128_CCM_SHA256 TLS_AES_128_GCM_SHA256

The TSF enforces the SCP-SGP22 secure channel for communication between U.SM-DP+ and S.ISD-R (ISD-R and SM-DP+). Identification of endpoints is addressed by the use of AES according to [GP AM F] using the parameters defined in [SGP.22], chapters 2.6 and 5.5, or in [SGP.32], chapters 2.6 and 5.5.

The TSF enforces SCP80 or SCP81 for communication between U.MNO-OTA and U.MNO-SD (MNO-SD and MNO OTA Platform). SCP80 must be provided to build secure channels to MNO OTA Platform (chapter 5.4 of [SGP.22] or chapter 5.4 of [SGP.32]). The TSF may also permit to use a SCP81 secure channel to perform the same functions than the SCP80 secure channel.

Applications may use the Secure Channel Protocol(s) supported by their associated Security Domain for securing information exchanged with the off-card entity (e.g. SCP02, SCP03).

Secure Channel Protocol 02 (SCP02) [GP] provides the three followings levels of security: entity authentication, integrity and data origin authentication and confidentiality. A further level of security applies to sensitive data (e.g. secret keys) that shall always be transmitted as confidential data. SCP02 is realised by the TOE based on the Triple-DES cryptographic algorithm.

Secure Channel Protocol 03 (SCP03) [GP AM D] provides the three followings level of security: mutual authentication, integrity and data origin authentication and confidentiality. It is based on SCP02 and is a secure channel protocol supporting AES-based cryptography. SCP03 is realized by the TOE based on the AES cryptographic algorithm.

The ITL component uses the AES GCM encryption scheme.

Secure Channel Protocol 11 (SCP11) [GP AM F] provides the three following levels of Security: mutual authentication, integrity and data origin authentication and confidentiality. It is based on Elliptic Curve Cryptography (ECC) for mutual authentication and secure channel initiation and on AES for secure messaging. SCP03 is realized by the TOE based on the AES cryptographic algorithm.

The cryptographic mechanisms used by the Secure Channel Protocols to enforce this protection and securely manage the associated keysets are provided by SF.CRYPTO.

This TSF is supported by SF.ACCESS_CONTROL that prevents reuse of authentication data related to the authentication mechanism used to open a secure communication channel.

7.7 SF.CRYPTO

This TSF controls all the operations related to the cryptographic key management (generation, distribution, destruction) and cryptographic operations (FCS_CKM.1/*, FCS_CKM.2/*, FCS_CKM.6/*, FCS_COP.1/*).

Key generation refers to the generation of a cryptographic key (for AES or Triple-DES) or key pair (for ECC) to be used in cryptographic algorithms.

Key destruction by physically overwriting keys with zero values is provided by the following means:

- The TOE zeroizes the session keys when closing the corresponding Secure Channel Session or upon card reset.

Key distribution is provided by the following means:

- PUT KEY, LoadBoundProfilePackage according to [GP] §11.8, [SGP.22] §5.7.6, [SGP.32] §5.9.8
- Profile download and installation according to [SGP.22] §3.1.3, §5.7.6, [SIMalliance], §8.6.3, [SIMalliance_2] §8.6.3.
- Profile download and installation according to [SGP.32] §3.2, §5.9.8, [SIMalliance] §8.6.3, [SIMalliance_2] §8.6.3

The TOE provides mechanisms for the authentication to the mobile networks via the algorithms MILENAGE, Tuak and Cave.

The TOE provides the following algorithms for hashing:

- SHA-256 as required by [SGP.22] §2.6.5: Hashing for digital signatures and hash-only applications, for HMAC, KDF and RNG, for the verification of the hash over the update image (after load phase completed) during the OS Update procedure.

The TOE provides the following algorithms for digital signature generation and verification:

- ECDSA is provided as required by the SFRs FDP_ACF.1/ECASD FIA_UAU.1/EXT (for U.SM-DP+ authentication), FIA_API.1.1, and [SGP.22] §2.6.7.2 signature computed as defined in [GP AM E] with one of the domain parameters in §2.6.7.1.

The TOE provides key agreement:

- ECKA-EG as required by the SFR FCS_CKM.1/SCP-SM and [SGP.22] §2.6.7.3; Annex G references [GP AM F] §3.1.1.

The TOE provides MAC generation and verification:

- Triple-DES CBC MAC as required by the SCP02 acc. to [GP] B.1.2.2 (Single DES plus final Triple-DES MAC)
- AES CBC MAC as required by the SRFs FIA_UAU.1/EXT (for U.MNO-OTA Authentication using SCP80 secure channel), FDP_IFF.1/SCP (SCP80/81, SCP-SGP.22), FDP_UIT.1/SCP, and by the Secure Channel Protocols SCP03 [GP AM D] and SCP80 [TS102 225], section 5.1.3.
- AES CMAC for SCP03 message authentication (FCS_COP.1/MAC_AES)
- AES CCM as required by TLS v1.3

The TOE provides encryption and decryption:

- Triple-DES in CBC mode as required by SCP02,
- AES in CBC mode as required by FDP_IFF.1/SCP (SCP80/81, SCP-SGP.22), FDP_UCT.1/SCP, SCP03.
- AES in GCM mode as required by TLS v1.3.
- AES in GCM mode used by OS Update procedure.

The TOE provides a cryptographic authentication mechanism based on the EID of the eUICC.

The cryptographic algorithms stated below of FCS_COP.1 are not provided as a service via JavaCard API.

7.8 SF.RNG

This security function is composed of random number generation that meets DRG.4 according [AIS20] (FCS_RNG.1). The random number generator provided by the TOE is a deterministic random bit generator based on the AES block cipher according to [ISO 18031].

Besides its use in key generation, applications may use the methods of the Java Card API javacard.security.RandomData class for generation of random numbers.

7.9 SF.IDENTITY

The TOE ensures that the eUICC is identified by a unique EID, based on the hardware identification of the eUICC (FIA_API.1).

The underlying IC used by the TOE is uniquely identified (FAU_SAS.1).

7.10 TSS Rationale

The justification and overview of the mapping between security functional requirements (SFR) and the TOE's security functionality (SF) is given in section above.

7.10.1 eUICC SFRs coverage

Security Functional Requirement	**Coverage by TSS Security Function(s)**
FIA_UID.1/EXT	SF.ACCESS_CONTROL
FIA_UAU.1/EXT	SF.ACCESS_CONTROL
FIA_USB.1/EXT	SF.ACCESS_CONTROL
FIA_UAU.4/EXT	SF.ACCESS_CONTROL
FIA_UID.1/MNO-SD	SF.ACCESS_CONTROL
FIA_USB.1/MNO-SD	SF.ACCESS_CONTROL
FIA_ATD.1/Base	SF.ACCESS_CONTROL
FIA_API.1.1	SF.IDENTITY
FDP_IFC.1/SCP	SF.SECURE_CHANNEL
FDP_IFF.1/SCP	SF.SECURE_CHANNEL
FTP_ITC.1/SCP	SF.SECURE_CHANNEL
FDP_ITC.2/SCP	SF.SECURE_CHANNEL
FPT_TDC.1/SCP	SF.ACCESS_CONTROL

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_UCT.1/SCP	SF.SECURE_CHANNEL
FDP_UIT.1/SCP	SF.SECURE_CHANNEL
FCS_CKM.1/SCP-SM	SF.CRYPTO
FCS_CKM.2/SCP-MNO	SF.CRYPTO
FCS_CKM.6/SCP-SM	SF.CRYPTO
FCS_CKM.6/SCP-MNO	SF.CRYPTO
FDP_ACC.1/ISDR	SF.ACCESS_CONTROL
FDP_ACF.1/ISDR	SF.ACCESS_CONTROL
FDP_ACC.1/ECASD	SF.ACCESS_CONTROL
FDP_ACF.1/ECASD	SF.ACCESS_CONTROL
FDP_IFC.1/Platform_services	SF.PLATFORM_MANAGEMENT
FDP_IFF.1/Platform_services	SF.PLATFORM_MANAGEMENT
FPT_FLS.1/Platform_services	SF.SECURITY
FCS_RNG.1	SF.RNG
FPT_EMS.1/Base	SF.SECURITY
FDP_SDI.1/Base	SF.INTEGRITY
FDP_RIP.1/Base	SF.SECURITY
FPT_FLS.1/Base	SF.SECURITY
FMT_MSA.1/PLATFORM_DATA	SF.ACCESS_CONTROL
FMT_MSA.1/RULES	SF.ACCESS_CONTROL

Security Functional Requirement	Coverage by TSS Security Function(s)
FMT_MSA.1/CERT_KEYS	SF.ACCESS_CONTROL
FMT_SMF.1/Base	SF.ACCESS_CONTROL
FMT_SMR.1/Base	SF.ACCESS_CONTROL
FMT_MSA.1/RAT	SF.ACCESS_CONTROL
FMT_MSA.3	SF.ACCESS_CONTROL
FCS_COP.1/Mobile_network	SF.CRYPTO
FCS_CKM.2/Mobile_network	SF.CRYPTO
FCS_CKM.6/Mobile_network	SF.CRYPTO

7.10.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	SF.ACCESS_CONTROL
FDP_ACF.1/FIREWALL	SF.ACCESS_CONTROL
FDP_IFC.1/JCVM	SF.ACCESS_CONTROL
FDP_IFF.1/JCVM	SF.ACCESS_CONTROL
FDP_RIP.1/OBJECTS	SF.SECURITY
FMT_MSA.1/JCRE	SF.ACCESS_CONTROL
FMT_MSA.1/JCVM	SF.ACCESS_CONTROL
FMT_MSA.2/FIREWALL_JCVM	SF.ACCESS_CONTROL
FMT_MSA.3/FIREWALL	SF.ACCESS_CONTROL

FMT_MSA.3/JCVM	SF.ACCESS_CONTROL
FMT_SMF.1/RE	SF.ACCESS_CONTROL
FMT_SMR.1/RE	SF.ACCESS_CONTROL
FCS_CKM.1 /ECC /Triple DES /AES	SF.CRYPTO
FCS_CKM.6/RE	SF.CRYPTO
FCS_COP.1 /SHA /SIG_ECC /MAC_TDES /MAC_AES /CIPH_TDES /CIPH_AES /CIPH_AES_GCM /ECKA-EG	SF.CRYPTO
FDP_RIP.1/ABORT	SF.TRANSACTION
FDP_RIP.1/APDU	SF.SECURITY
FDP_RIP.1/bArray	SF.SECURITY
FDP_RIP.1/GlobalArray	SF.SECURITY
FDP_RIP.1/KEYS	SF.SECURITY
FDP_RIP.1/TRANSIENT	SF.SECURITY
FDP_ROL.1/FIREWALL	SF.TRANSACTION
FAU_ARP.1	SF.SECURITY

FDP_SDI.2/DATA	SF.INTEGRITY
FPR_UNO.1	SF.SECURITY
FPT_FLS.1/RE	SF.SECURITY
FPT_TDC.1/RE	SF.ACCESS_CONTROL
FIA_ATD.1/AID	SF.ACCESS_CONTROL
FIA_UID.2/AID	SF.ACCESS_CONTROL
FIA_USB.1/AID	SF.ACCESS_CONTROL
FMT_MTD.1/JCRE	SF.ACCESS_CONTROL
FMT_MTD.3/JCRE	SF.ACCESS_CONTROL
FDP_ACC.2/ADEL	SF.ACCESS_CONTROL
FDP_ACF.1/ADEL	SF.ACCESS_CONTROL
FDP_RIP.1/ADEL	SF.SECURITY
FMT_MSA.1/ADEL	SF.ACCESS_CONTROL
FMT_MSA.3/ADEL	SF.ACCESS_CONTROL
FMT_SMF.1/ADEL	SF.ACCESS_CONTROL
FMT_SMR.1/ADEL	SF.ACCESS_CONTROL
FPT_FLS.1/ADEL	SF.SECURITY
FDP_RIP.1/ODEL	SF.SECURITY
FPT_FLS.1/ODEL	SF.SECURITY
FCO_NRO.2/GP	SF.SECURE_CHANNEL
FIA_AFL.1/GP	SF.SECURE_CHANNEL
FIA_UAU.1/GP	SF.ACCESS_CONTROL

FIA_UAU.4/GP	SF.ACCESS_CONTROL
FDP_UIT.1/GP	SF.SECURE_CHANNEL
FDP_UCT.1/GP	SF.SECURE_CHANNEL
FDP_IFC.2/GP-KL	SF.SECURE_CHANNEL
FDP_IFC.2/GP-ELF	SF.SECURE_CHANNEL
FMT_MSA.3/GP	SF.ACCESS_CONTROL
FMT_MSA.1/GP	SF.ACCESS_CONTROL
FMT_SMR.1/GP	SF.ACCESS_CONTROL
FDP_ITC.2/GP-KL	SF.ACCESS_CONTROL
FDP_ITC.2/GP-ELF	SF.ACCESS_CONTROL
FPT_FLS.1/GP	SF.SECURITY
FPT_RCV.3/GP	SF.TRANSACTION
FTP_ITC.1/GP	SF.SECURE_CHANNEL
FDP_IFF.1/GP-ELF	SF.SECURE_CHANNEL
FDP_IFF.1/GP-KL	SF.SECURE_CHANNEL
FMT_SMF.1/GP	SF.ACCESS_CONTROL
FIA_UID.1/GP	SF.SECURE_CHANNEL
FPT_TDC.1/GP	SF.ACCESS_CONTROL
FDP_ROL.1/GP	SF.TRANSACTION

7.10.3 Secure IC SFRs coverage

Security Functional Requirement	**Coverage by TSS Security Function(s)**
FAU_SAS.1	SF.IDENTITY
FPT_PHP.3	SF.SECURITY
FPT_RCV.3/OS	SF.SECURITY
FPT_RCV.4.1/OS	SF.SECURITY

7.10.4 OS Update (ITL) SFRs coverage

Security Functional Requirement	**Coverage by TSS Security Function(s)**
FDP_ACC.1/OS-UPDATE	SF.ACCESS_CONTROL
FDP_ACF.1/OS-UPDATE	SF.ACCESS_CONTROL
FMT_MSA.3/OS-UPDATE	SF.ACCESS_CONTROL
FMT_SMF.1/OS-UPDATE	SF.ACCESS_CONTROL
FMT_SMR.1/OS-UPDATE	SF.ACCESS_CONTROL
FCS_COP.1/OS-UPDATE-DEC	SF.CRYPTO
FCS_COP.1/OS-UPDATE-VER	SF.CRYPTO
FIA_ATD.1/OS-UPDATE	SF.ACCESS_CONTROL
FTP_TRP.1/OS-UPDATE	SF.SECURE_CHANNEL
FPT_FLS.1/OS-UPDATE	SF.SECURITY

7.10.5 Association table of SFRs and TSS

TSF	SFR
SF.TRANSACTION	FDP_ROL.1/FIREWALL FPT_RCV.3/GP FDP_RIP.1/ABORT FDP_ROL.1/GP FPT_RCV.3/GP
SF.ACCESS_CONTROL	FIA_UID.1/EXT FIA_UAU.1/EXT FIA_USB.1/EXT FIA_UAU.4/EXT FIA_UID.1/MNO-SD FIA_USB.1/MNO-SD FIA_ATD.1/Base FPT_TDC.1/SCP FDP_ACC.1/ISDR FDP_ACF.1/ISDR FDP_ACC.1/ECASD FDP_ACF.1/ECASD FMT_MSA.1/PLATFORM_DATA FMT_MSA.1/RULES FMT_MSA.1/CERT_KEYS FMT_SMF.1/Base FMT_SMR.1/Base FMT_MSA.1/RAT FMT_MSA.3 FDP_ACC.2/FIREWALL FDP_ACF.1/FIREWALL

	FDP_IFC.1/JCVM FDP_IFF.1/JCVM FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_MSA.2/FIREWALL_JCVM FMT_MSA.3/FIREWALL FMT_MSA.3/JCVM FDP_ITC.2GP-ELF FMT_SMR.1GP FDP_ACC.2/ADEL FDP_ACF.1/ADEL FMT_MSA.1/ADEL FMT_MSA.3/ADEL FMT_SMF.1/ADEL FMT_SMR.1/ADEL FMT_SMF.1/GP FMT_SMR.1/GP FMT_MSA.1/GP FMT_MSA.3/GP FIA_UAU.1/GP FIA_UAU.4/GP FDP_ITC.2/GP-KL FDP_ITC.2/GP-ELF FPT_TDC.1/GP FMT_SMR.1/RE FMT_SMF.1/RE FPT_TDC.1/RE FIA_ATD.1/AID

	FIA_UID.2/AID FIA_USB.1/AID FMT_MTD.1/JCRE FMT_MTD.3/JCRE FMT_MSA.3/OS-UPDATE FMT_SMF.1/OS-UPDATE FMT_SMR.1/OS-UPDATE FDP_ACC.1/OS-UPDATE FDP_ACF.1/OS-UPDATE FIA_ATD.1/OS-UPDATE
SF.INTEGRITY	FDP_SDI.1/Base FDP_SDI.2/DATA
SF.SECURITY	FPT_FLS.1/Platform_services FPT_EMS.1/Base FDP_RIP.1/Base FPT_FLS.1/Base FDP_RIP.1/OBJECTS FDP_RIP.1/APDU FDP_RIP.1/bArray FDP_RIP.1/GlobalArray FDP_RIP.1/KEYS FDP_RIP.1/TRANSIENT FAU_ARP.1 FPR_UNO.1 FPT_FLS.1/RE FPT_FLS.1GP FPT_FLS.1/ADEL FPT_FLS.1/ODEL

	FDP_RIP.1/ADEL FDP_RIP.1/ODEL FPT_PHP.3 FPT_FLS.1/GP FPT_FLS.1/OS-UPDATE
SF.PLATFORM_MANAGEMENT	FDP_IFC.1/Platform_services FDP_IFF.1/Platform_services
SF.SECURE_CHANNEL	FDP_IFC.1/SCP FDP_IFF.1/SCP FTP_ITC.1/SCP FDP_ITC.2/SCP FDP_UCT.1/SCP FDP_UIT.1/SCP FCO_NRO.2/GP FIA_AFL.1/GP FDP_IFC.2/GP-KL FDP_IFC.2/GP-ELF FDP_IFF.1/GP-KL FDP_IFF.1/GP-ELF FDP_UIT.1/GP FDP_UCT.1/GP FIA_UID.1/GP FTP_ITC.1/GP FCO_NRO.2/GP FTP_TRP.1/OS-UPDATE
SF.CRYPTO	FCS_CKM.1/SCP-SM FCS_CKM.2/SCP-MNO FCS_CKM.6/SCP-SM

	FCS_CKM.6/SCP-MNO FCS_COP.1/Mobile_network FCS_CKM.2/Mobile_network FCS_CKM.6/Mobile_network FCS_CKM.1/ECC FCS_CKM.1/Triple DES FCS_CKM.1/AES FCS_CKM.6/RE FCS_COP.1/SHA FCS_COP.1/SIG_ECC FCS_COP.1/MAC_TDES FCS_COP.1/MAC_AES FCS_COP.1/CIPH_TDES FCS_COP.1/CIPH_AES FCS_COP.1/CIPH_AES_GCM FCS_COP.1/ECKA-EG FCS_COP.1/OS-UPDATE-DEC FCS_COP.1/OS-UPDATE-VER
SF.RNG	FCS_RNG.1
SF.IDENTITY	FIA_API.1 FAU_SAS.1

8. Statement of Compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST). This statement is compliant to the requirements of [SUPP].

8.1 Classification of the Platform TSFs

A classification of TSFs of the Platform-ST has been made. Each TSF has been classified as 'relevant' or 'not relevant' for the Composite-ST.

Chapter in [IC_ST] and [IC 2_ST]	TOE Security Functionality	Relevant	Not relevant
6.1	Limited fault tolerance (FRU_FLT.2)	x	
6.2	Failure with preservation of secure state (FPT_FLS.1)	x	
6.3	Limited capabilities (FMT_LIM.1) / Sdiag, Limited capabilities (FMT_LIM.1) / Loader, Limited capabilities (FMT_LIM.1) / Test, Limited availability (FMT_LIM.2) / Sdiag & Limited availability (FMT_LIM.2) / Loader, Limited availability (FMT_LIM.2) / Test		x
6.4	Inter-TSF trusted channel (FTP_ITC.1) / Sdiag		x
6.5	Audit review (FAU_SAR.1) / Sdiag		x
6.6	Stored data confidentiality (FDP_SDC.1)	x	
6.7	Stored data integrity monitoring and action (FDP_SDI.2)	x	
6.8	Audit storage (FAU_SAS.1)	x	
6.9	Resistance to physical attack (FPT_PHP.3)	x	
6.10	Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1)	x	
6.11	Random number generation (FCS_RNG.1) / PTG.2	x	
6.12	Cryptographic operation: DES operation (FCS_COP.1) / DES	x	
6.13	Cryptographic operation: AES operation (FCS_COP.1) / AES	x	
6.14	Static attribute initialisation (FMT_MSA.3) / Memories	x	
6.15	Management of security attributes (FMT_MSA.1) / Memories & Specification of management functions (FMT_SMF.1) / Memories	x	

6.16	Complete access control (FDP_ACC.2) / Memories & Security attribute based access control (FDP_ACF.1) / Memories	x	
6.17	Authentication Proof of Identity (FIA_API.1)		x
6.18	Inter-TSF trusted channel (FTP_ITC.1) / Loader, Basic data exchange confidentiality (FDP_UCT.1) / Loader, Data exchange integrity (FDP_UIT.1) / Loader & Audit storage (FAU_SAS.1) / Loader		x
6.19	Subset access control (FDP_ACC.1) / Loader & Security attribute based access control (FDP_ACF.1) / Loader		x
6.20	Failure with preservation of secure state (FPT_FLS.1) / Loader		x
6.21	Static attribute initialisation (FMT_MSA.3) / Loader		x
6.22	Management of security attributes (FMT_MSA.1) / Loader & Specification of management functions (FMT_SMF.1) / Loader		x
6.23	Security roles (FMT_SMR.1) / Loader		x
6.24	Timing of identification (FIA_UID.1) / Loader & Timing of authentication (FIA_UAU.1) / Loader		x
6.25	Audit review (FAU_SAR.1) / Loader		x

Table 29 Classification of Platform-TSFs

The TSFs related the Loader are not relevant, because the Loader functionality is permanently disabled before TOE delivery.

The TSFs related to Secure Diagnostics are not relevant for the Composite ST, because the functionality is not used by the TOE and is permanently disabled.

8.2 Matching statement

The TOE relies on fulfilment of the following implicit assumptions on the IC:

- Certified microcontroller ST33K1M5C, ST33K1M5A and ST33K1M5M.
- True Random Number Generation with PTG.2 classification according to [AIS31].
- Cryptographic support based on symmetric key algorithms AES with 128, 192, 256 bits key length and Triple DES with 112, 168 bits key length.

- Cryptographic support based on asymmetric key algorithm ECDSA with up to 512 bits elliptic curve key length, including key generation.

The rationale of the Platform-ST has been used to identify the relevant SFRs, TOE objectives, threats and OSPs. All SFRs, objectives for the TOEs, but also all objectives for the TOE-environment, all threats and OSPs of the Platform-ST have been used for the following analysis.

8.3 Security objectives

This Composite-ST has security objectives which are related to the Platform-ST. These are:

- O.IC.SUPPORT
- O.IC.RECOVERY
- O.IC.PROOF-OF-IDENTITY

The following platform objectives could be mapped to composite objectives:

- BSI.O.Leak-Inherent
- BSI.O.Phys-Probing
- BSI.O.Malfunction
- BSI.O.Phys-Manipulation
- BSI.O.Leak-Forced
- BSI.O.Abuse-Func
- BSI.O.Identification
- BSI.O.RND
- AUG1.O.Add-Functions
- AUG4.O.Mem-Access

These Platform-ST objectives can be mapped to the Composite-ST objectives as shown in the following table.

Platform ST Objective	Correspondence in Composite ST		
	O.IC.SUPPORT	O.IC.RECOVERY	O.IC.PROOF-OF-IDENTITY
BSI.O.Leak-Inherent	X		
BSI.O.Phys-Probing	X		
BSI.O.Malfunction	X	X	
BSI.O.Phys-Manipulation	X		
BSI.O.Leak-Forced	X		
BSI.O.Abuse-Func	X		
BSI.O.Identification	X		X
BSI.O.RND	X		
AUG1.O.Add-Functions	X		
AUG4.O.Mem-Access	X		

O.IC.RECOVERY matches to BSI.O.Malfunction because this allows the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.

O.IC.SUPPORT matches the listed objectives of the Platform-ST because they provide functionality that supports (1) safeguarding the access to low-level functions (incl. protection against disclosure or modification of private data and code), the well-functioning of the TSFs of the TOE (avoiding they are bypassed or altered), (2) secure low-level cryptographic processing and random number generation, (3,4) the TOEs memory model and operations (allowing to store data in “persistent technology memory” or in volatile memory and performing memory operations atomically).

O.IC.PROOF-OF-IDENTITY meets BSI.O.Identification from the Platform-ST because it provides capability of the TOE to store Initialisation Data and/or Pre-personalisation Data according to FAU_SAS.1. The Initialisation Data (or parts of them) are used for TOE identification.

The following Platform-ST objectives are not relevant for or cannot be mapped to the Composite-TOE:

- JIL.O.TOE-Identification, BSI.O.Cap-Avail-Loader and BSI.O.Ctrl-Auth-Loader are not relevant because the Composite-TOE is delivered only with disabled Loading capability.
- BSI.O.Authentication is not relevant, since it is not available after TOE delivery.
- JIL.O.Prot-TSF-Confidentiality is not relevant because the Composite-TOE is delivered only with disabled Loading capability (irreversible operation) and not delivered as an open sample.
- JIL.O.Secure-Load-ACode is not relevant because the Composite-TOE does not use “Secure loading of Additional Code”.
- JIL.O.Secure-AC-Activation is not relevant because the Composite-TOE does not use “Secure activation of Additional Code”.
- O.Secure-Load-AMemImage is not relevant because the Composite-TOE does not use “Secure loading of Additional Memory Image”.
- O.MemImage-Identification is not relevant because the Composite-TOE does not use “Secure identification of Memory Image”.
- O.Firewall is not relevant because the TOE does not support the specific application and therefore, the specific application firewall is not used.

There is no conflict between security objectives of this Composite-ST and the Platform-ST [IC_ST] / [IC 2_ST].

8.4 Security objectives for the environment

Platform ST Sec. Obj. Env.	**Correspondence in Composite ST**	
	Relevant	TOE ST Sec. Objective
BSI.OE.Resp-Appl	Yes	O.RE.SECURE-COMM, O.RE.PRE-PPI, O.RE.IDENTITY, O.API, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.SECURE_LOAD_ACODE, O.CONFID-UPDATE-IMAGE.LOAD
BSI.OE.Process-Sec-IC	No	N/A
BSI.OE.Lim-Block-Loader	No	N/A
BSI.OE.Loader-Usage	No	N/A
BSI.OE.TOE-Auth	Yes	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS
OE.Composite-TOE-Id	Yes	O.PROOF_OF_IDENTITY
OE.TOE-Id	Yes	O.IC.PROOF_OF_IDENTITY
OE.Enable-Disable-Secure-Diag	No	N/A
OE.Secure-Diag-Usage	No	N/A

The table above shows the following:

- Column “Platform ST Sec. Obj. Env.” lists the Security Objectives for the Operational Environment from the Platform ST.
- Column “Relevant” specifies for each security objective if it is relevant for the composite certification or not.

- Column “TOE ST Sec. Objective” maps the security objectives for the TOE from Composite-ST to each relevant security objective for the operational environment from Platform-ST.

BSI.OE.Lim-Block-Loader Loader is not relevant because the Composite-TOE is delivered only with disabled Loading capability.

BSI.OE.Loader-Usage Loader is not relevant because the Composite-TOE is delivered only with disabled Loading capability.

BSI.OE.Process-Sec-IC Protection during composite product manufacturing is assured by the aspects of the assurance class ALC.

OE.Enable-Disable-Secure-Diag is not relevant because the Secure Diagnostic capability is disabled.

OE.Secure-Diag-Usage is not relevant because the Secure Diagnostic capability is disabled.

8.5 Security requirements

8.5.1 Security Functional Requirements

Platform SFR	**Correspondence in Composite ST**
FRU_FLT.2	FPT_RCV.3
FPT_FLS.1	FPT_FLS.1/*, FPT_RCV.3
FMT_LIM.1/Test	Internal test features of the IC platform are not accessible by the Composite TOE.
FMT_LIM.2/Test	Internal test features of the IC platform are not accessible by the Composite TOE.

FMT_LIM.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_LIM.2/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_LIM.1/Sdiag	Not used by the composite SFRs
FMT_LIM.2/Sdiag	Not used by the composite SFRs
FAU_SAS.1	FAU_SAS.1
FDP_SDC.1	FPT_PHP.3, FPT_EMS.1/Base
FDP_SDI.2	FDP_SDI.2/DATA
FPT_PHP.3	FPT_PHP.3, FPT_EMS.1/Base
FDP_ITT.1	FDP_IFC.1.1/JCVM
FPT_ITT.1	FDP_ACF.1/FIREWALL, FPT_EMS.1/Base
FDP_IFC.1	FDP_IFC.1/JCVM, FDP_IFC.2/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFC.1/Platform_services, FPT_EMS.1/Base
FCS_RNG.1/PTG.2	FCS_RNG.1.1, PTG.2 is used as input for DRG.4.
FCS_COP.1/DES	EDES+ accelerator is used for Triple DES operations of FCS_COP.1/CIPH_TDES.
FCS_COP.1/AES	AES accelerator is used for AES operations of FCS_COP.1/CIPH_AES_*.
FDP_ACC.2/Memories	FDP_ACC.2/FIREWALL, FDP_ACC.2/ADEL
FDP_ACF.1/Memories	FDP_ACF.1/FIREWALL, FDP_ACF.1/ADEL, FDP_ACF.1/ECASD, FDP_ACF.1/ISDR, FDP_ACF.1/OS-UPDATE

FMT_MSA.1/Memories	FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.1/ADEL, FMT_MSA.1/GP, FMT_MSA.1/RAT, FMT_MSA.1/CERT_KEYS, FMT_MSA.1/PLATFORM_DATA
FMT_MSA.3/Memories	FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MSA.3/ADEL, FMT_MSA.3/GP, FMT_MSA.3, FMT_MSA.3/OS-UPDATE
FMT_SMF.1/Memories	FMT_SMF.1, FMT_SMF.1/ADEL, FMT_SMF.1/GP, FMT_SMF.1/OS-UPDATE
FIA_API.1	Nor relevant, since the TOE is delivered in User configuration.
FTP_ITC.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_UCT.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_UIT.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_ACC.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_ACF.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_MSA.3/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_MSA.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_SMR.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.

FIA_UID.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FIA_UAU.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_SMF.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FPT_FLS.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FAU_SAS.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FAU_SAR.1/Loader	Not relevant, since the Flash Loader is permanently deactivated.
FTP_ITC.1/Sdiag	Not used by the composite SFRs
FAU_SAR.1/Sdiag	Not used by the composite SFRs

8.5.2 Security Assurance Requirements

The Composite-ST requires EAL 4 according to Common Criteria V3.1 R5 augmented by ALC_DVS.2 and AVA_VAN.5

The Platform-ST has been certified to EAL 6 according to Common Criteria V3.1 R5 augmented by: ALC_FLR.1.

The assurance requirements of the Composite-ST represent a subset of the assurance requirements of the Platform-ST.

9. References

[3GPPAuth] 3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture, version 12.2.0, release 12, December 2014. 3GPP TS 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, version 12.16.0, release 12, December 2015.

[419 212] 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.

[AGD_PRE] Preparative Procedures for Sm@rtSIM Polaris SGP.22/SGP.32 (confidential document), Version 1.6, 26.02.2025

Sm@rtSIM Next Generation v2.0 ATR and CPLC, Version 1.1, 14.11.2024

[AGD_OPE] Sm@rtSIM Polaris SGP.22/SGP.32, API Support (confidential document), Version 2.1, 11.10.2024

OS Update – Customer Guidelines (confidential document), Version 2.4, 26.01.2024

[AGD_SEC] Security Guidance for Sm@rtSIM Polaris SGP.22/SGP.32 (confidential document), Version 1.3, 11.03.2025

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20, Version 3, 15.05.2013, Funktionalitätsklassen und Evaluierungsmethodologie für deterministische Zufallszahlengeneratoren, Zertifizierungsstelle des BSI.

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Funktionalitätsklassen und Evaluierungsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013

[ANSIX962] ANSI X9.62:2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)

[BSI TR 03111] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography Version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[CAVE] TR45.AHAG, Common Cryptographic Algorithms, Revision D, Publication Version, March 14, 2000

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version CC:2022 Revision 1, November 2022.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version CC:2022 Revision 1, November 2022.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version CC:2022 Revision 1, November 2022.

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, version CC:2022 Revision 1, November 2022.

[FIPS46-3] Federal Information Processing Standards PUB 46-3, Data Encryption Standard, reaffirmed 1999 October 25

[FIPS180-4] Federal Information Processing Standards Publication 180-4, Secure Hash Standard, March 2012

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4 DIGITAL SIGNATURE STANDARD (DSS) (with Change Notice), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, July 2013

[FIPS197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[GP] GlobalPlatform Card Specification, Version 2.3.1

[GP AM B] GlobalPlatform Card Specification v2.3 Amendment B – Remote Application Management over HTTP, Version 1.2, March 2022.

[GP AM D] GlobalPlatform Card Specification v2.3 Amendment D – Secure Channel Protocol 03, Version 1.2, April 2020

[GP AM E] GlobalPlatform Card Specification v2.2 Amendment E – Security Upgrade for Card Content Management, Version 1.0.1, July 2014.

[GP AM F] GlobalPlatform Card Specification v2.2 Amendment F – Secure Channel Protocol ‘11’, Version 1.0, May 2015.

[GP UICC] GlobalPlatform Card, UICC Configuration, Version 2.0, November 2015

[GP SG] GlobalPlatform Card Composition Model Security Guidelines for

Basic Applications, Version 2.0, December 2014.

[ICAO 9303] Machine Readable Travel Documents, 7th edition 2015.

[ISO 9796-2] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002

[ISO 9797-1] ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

[ISO 18031] ISO/IEC 18031:2011: Information technology — Security techniques — Random bit generation

[ISO 15946] ISO/IEC 15946-5:2009, Cryptographic techniques based on elliptic curves

[JCAPI], [JCAPI3] Java Card Platform, versions 3.0 up to 3.1, Classic Edition, Application Programming Interface. Published by Oracle.

[JCRE], [JCRE3] Java Card Platform, versions 3.0 up to 3.1, Classic Edition, Application Programming Interface. Published by Oracle.

[JCVM], [JCVM3] Java Card Platform, versions 3.0 up to 3.1, Classic Edition, Virtual Machine (Java Card VM) Specification. Published by Oracle.

[JCVM22] Java Card Platform, version 2.2 Virtual Machine (Java Card VM) Specification. June 2002. Published by Sun Microsystems, Inc.

[MILENAGE] 3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 11): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General; Document 2: Algorithm Specification; Document 3: Implementers Test Data; Document 4: Design Conformance Test Data; Document 5: Summary and results of design and evaluation.

[PKCS1] PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note, Version 2.1, February, 2003.

[PKCS3] PKCS#3: Diffie-Hellman Key Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993.

[PP-JCS] Java Card Protection Profile - Open Configuration, April 2020, Version 3.1, (Oracle)

[PP-GP] GlobalPlatform Technology – Secure Element Protection Profile, Version 1.0, February 2021, Document Reference: GPC_SPE_174

[PP0084] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, February 2014, BSI-CC-PP-0084-2014.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, DOI 10.17487/RFC1321, April 1992, <https://www.rfc-editor.org/info/rfc1321>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: KeyedFDP_.1-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, DOI 10.17487/RFC3447, February 2003, <https://www.rfc-editor.org/info/rfc3447>.

[RFC5639] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, DOI 10.17487/RFC5639, March 2010, <https://www.rfc-editor.org/info/rfc5639>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[SGP.02] Remote Provisioning Architecture for Embedded UICC Technical Specification

- Version 2.0, October 2014
- Version 3.0, June 2015
- Version 4.2, July 2020
- Version 4.3, January 2023

References to [SGP.02] in this ST may be interpreted as any of the three versions of this document.

References to [SGP.02] version 2.0 (respectively [SGP.02] version 3.0) shall be interpreted as only the version 2.0 (respectively 3.0) of the document.

[SGP.21] Remote SIM Provisioning (RSP) Architecture, version 2.5, GMSA Association, 11 November 2022.

[SGP.22] RSP Technical Specification, GSM Association, Version 2.5, 25 May 2023.

[SGP.31] Remote SIM Provisioning (RSP) Architecture, version 1.2, GMSA Association, 26 April 2024.

[SGP.32] RSP Technical Specification, GSM Association, Version 1.2, 27 June 2024.

[SGP.17] SGP.17-1 Security Target Template for Consumer eUICC, Version 1.0, 05 July 2023, GSM Association

[PP-eUICC] Embedded UICC for Consumer Devices Protection Profile, GSM Association, Version 2.1, 03 February 2025.

[SIMalliance] SIMalliance eUICC Profile Package: Interoperable Format Technical Specification V2.3.1.

[SIMalliance_2] SIMalliance eUICC Profile Package: Interoperable Format Technical Specification V3.3.1.

[SP800-38a] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001.

[SP800-38b] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005.

[SP800-38d] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, 2007.

[SP800-67] National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, version 1.2, July 2011.

[SP800-90A] National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, January 2012.

[SUPP] Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, May 2018, Version 1.5.1.

[TS102 223] ETSI TS 102 223 V15.1.0 (2019-02), Smart Cards; Card Application Toolkit (CAT) (Release 15).

[TS102 225] ETSI TS 102 225 V16.0.0 (2020-06), Smart Cards; Secured packet structure for UICC based applications (Release 16).

[TS102 226] ETSI TS 102 226 V16.0.0 (2020-07), Smart Cards; Remote APDU structure for UICC based applications (Release 16).

[Tuak] 3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0, release 12, December 2014. Document 1: Algorithm specification; Document 2: Implementers' test data; Document 3: Design conformance test data.

[IC_ST] ST33K1M5C and ST33K1M5T C02 Security Target for composition, SMD_ST33K1M5_ST_21_001 Rev C02.1, August 2024, STMicroelectronics.

[IC 2_ST] ST33K1M5A and ST33K1M5M B03 Security Target for composition, SMD_ST33K1M5AM_ST_21_002 Rev B03.1, August 2024, STMicroelectronics.

[DCG] Certification Report BSI-DSZ-CC-S-0185-2021-MA-01 for Giesecke+Devrient Mobile Security Development Center Germany (DCG), 4 October 2021 (Certificate Date), Bundesamt für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/Standortzertifizierung/S_0185.html

[DCI] Certification Report CCN-CC/2022-20/INF-3991 for Giesecke+Devrient Development Center India (DCI), related to CCN-CC-1/2023, 19 January 2023 (Certificate Date), National Cryptologic Centre (CCN). https://oc.ccn.cni.es/productos-certificados/centros-certificados/437-g-d-development-center-india-dci

[DCS] Certification Report CCN-CC/2022-53/INF-4095 for Giesecke+Devrient Development Center Spain (DCS), related to CCN-CC-15/2023, 17 May 2023 (Certificate Date), National Cryptologic Centre (CCN). https://oc.ccn.cni.es/productos-certificados/centros-certificados/689-giesecke-devrient-development-center-spain-dcs

Maintenance Report 2023-21_INF-4149 for Giesecke+Devrient Development Center Spain (DCS), 28.07.2023

[GDIMS] Certification Report CCN-CC/2024-08/INF-4392 for Giesecke + Devrient ePayments Iberia, related to CCN-CC-18/2024, 06 September 2024 (Certificate Date), National Cryptologic Centre (CCN). https://oc.ccn.cni.es/productos-certificados/centros-certificados/1024-giesecke-devrient-epayments-iberia?ic=1

[NAN] Certification Report CCN-CC/2023-26/INF-4297 for

Giesecke+Devrient (Jiangxi) Technology GDCNMS NAN, related to CCN-CC-6/2024, 22 March 2024 (Certificate Date), National Cryptologic Centre (CCN). https://oc.ccn.cni.es/productos-certificados/centros-certificados/1010-giesecke-devrient-jiangxi-technology-co-ltd-gdcnms-nan

List of tables