Giesecke+Devrient

Public Security Target

Sm@rtSIM® Tabit800

Consumer/M2M SGP.32

Department: MS Security

Author: G+D Mobile Security Germany GmbH

Version: 1.1

Date: 23.07.2026

Status: Released

Classification: PUBLIC

History

Version	Date	Author	Description of change
1.0	08.07.2026	G+D MS	Released version (public)
1.1	23.07.2026	G+D MS	References in section 11

Table 1. History

Contents

1. Security Target Introduction

1.1 Security Target reference

Name	Public Security Target Sm@rtSIM® Tabit800 Consumer/M2M SGP.32
Version	1.1
Date	23.07.2026
Author	Giesecke+Devrient Mobile Security Germany GmbH
Reference	GDI_Tabit800_SGP32_ASE_1.1_public

Table 2. Security Target reference

1.2 TOE reference

Name	Sm@rtSIM® Tabit800 Consumer/M2M SGP.32
Version	1.0
Reference	Sm@rtSIM® Tabit800 Consumer/M2M SGP.32

Table 3. TOE reference

Consumer and M2M refer to the hardware grades, as the TOE implements SGP.32 (IoT) only. See section 2.1 for details.

2. TOE overview

2.1 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, in “Consumer” and “M2M” hardware grades as referenced in the TOE Name (section 1.2).
- The OS
- The Runtime Environment (the Java Card System), version 3.1
- The GlobalPlatform Card Content Management, version 2.3.1 plus **[GP AM B]** 1.2, **[GP AM D]** 1.2, **[GP AM E]** 1.1.

The TOE implements the GSMA eSIM IoT Architecture and Requirements for IoT Devices only: **[SGP.31]**, **[SGP.32]** and **[SGP.33-1]**. A detailed TOE overview is given in chapter 1.2 of **[PP-eUICC]**.

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.

2.2 TOE type and usage

The TOE type is a composite of secure software implemented on secure IC.

The eUICC is an UICC embedded in an IoT device. The eUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile. The Profiles are not part of the TOE.

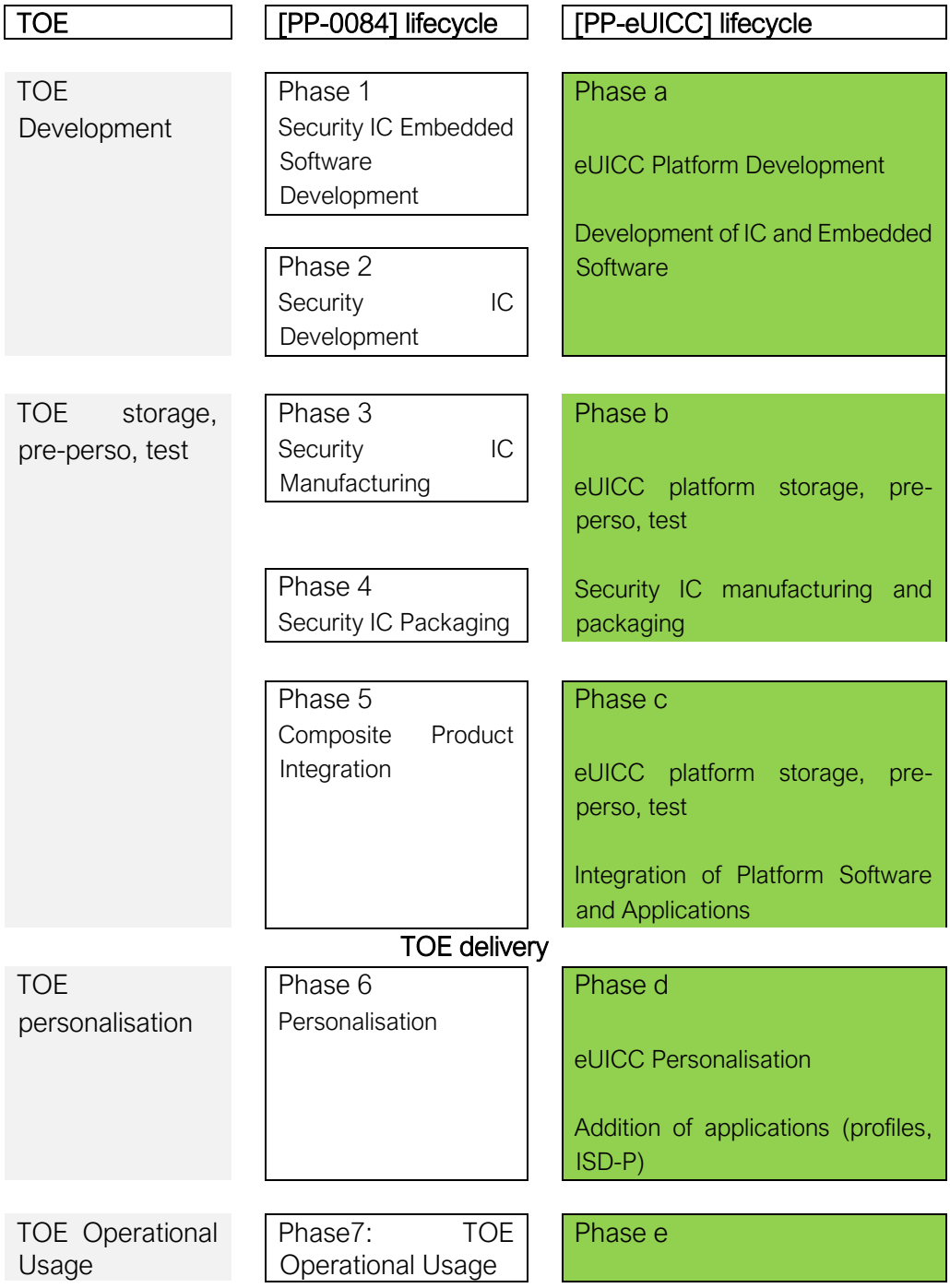
The TOE relies on IoT Profile Assistant (IPA), a software running in the device introduced and defined in the [SGP.31], [SGP.32] and [SGP.33-1] specifications. This is implemented as a non-TOE on-device until called IPAd.

In this product, IPAe is not part of the TOE.

2.3 TOE life cycle

Based on [PP-eUICC], the life-cycle of the TOE is composed of 5 phases where its delivery happens at the end of the eUICC lifecycle Phase c as shown and described in Table 4.

The TOE is self-protected at the end of the eUICC lifecycle Phase d.



		eUICC integration, delivery of product to end-user eUICC remote provisioning

Table 4 TOE life-cycle phases and TOE delivery

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

Non-TOE is same than the ones mentioned in **[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.

2.4 TOE scope

2.4.1 Physical scope

Category	Component	Version	Delivery form
HW	CC Certificate: BSI-DSZ-CC-1126-V4-2025 - SLM17ECB800B - SLC17ECB800B	design step: - M31 - T31	Diced wafer via courier delivery
FW	SLx17 firmware	80.301.05.1	Binary in memory
SW	Sm@rtSIM® Tabit800 Consumer/M2M SGP.32	1.0	Binary in memory
DOC	Operative guidance	[AGD_OPE]	Pdf file via secure email (PGP encrypted)
DOC	Preparative guidance	[AGD_PRE]	Pdf file via secure email (PGP encrypted)
DOC	Security guidance	[AGD_SEC]	Pdf file via secure email (PGP encrypted)

Table 5. TOE Physical scope

2.4.2 Logical scope

The TOE is a composite of eUICC OS implemented on a certified IC, as described in the section 2.1 of this ST.

The eUICC OS is composed by: Application Layer and Platform Layer. These layers are described in [PP-eUICC], section 1.2.1.

The logical boundaries are delimited with a red line in Figure 1:

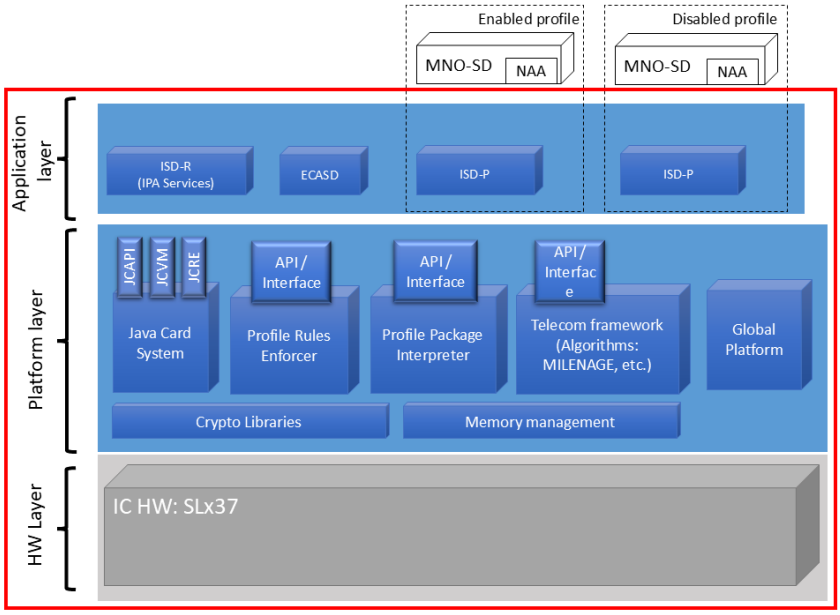


Figure 1 TOE Logical Scope

3. Conformance Claim

3.1 Common Criteria version and conformance with CC part 2 and part 3

The Security Target conforms to Common Criteria 2022 Release 1:

- CC Part 1 [CC1]
- CC Part 2 [CC2] (Extended),
- CC Part 3 [CC3] (conformant),

[CC-ERRATA] has been taken into account.

The extended Security Functional Requirements are defined in section 6.

3.2 CC Part 5 [CC5]. Assurance package

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5. Due to the product being a composite, it also conforms to Composite product package (COMP) defined in section 6 of [CC5].

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

3.3 Protection Profile (PP) conformance claim

This Security Target claims demonstrable conformance to the [PP-eUICC] protection profile: Base-PP.

3.4 Conformance claim rationale

Conformance rationale of the ST against [PP-eUICC] is mapped below. The conformance rationale focuses on assets, threats, OSPs, assumptions, security objectives, and SFRs and the notation used is detailed below:

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

- Refinement (R): The element in the ST refines the corresponding [PP-eUICC] element. New names are given between brackets and added to the list of elements.
- Addition (A): The element is newly defined in the ST; it is not present in [PP-eUICC] and does not affect it.
- Deletion (D): The element is deleted from [PP-eUICC].
- X: The element is present in [PP-eUICC].

3.4.1 Conformity of the TOE Type

The TOE follows the third scenario from the definition in [PP-eUICC] 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.

3.4.2 SPD Consistency

3.4.2.1 Assets consistency

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

All assets are described in section 4.1.

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.PROFILE_USER_CODES (SGP.22)	X	(D) : this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only.
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_CODE		(A): Added from [PP-JCS].
D.APP_C_DATA		(A): Added from [PP-JCS].
D.APP_I_DATA		(A): Added from [PP-JCS].
D.APP_KEYs		(A): Added from [PP-JCS].
D.PIN		(A): Added from [PP-JCS].
D.API_DATA		(A): Added from [PP-JCS].
D.CRYPTO		(A): Added from [PP-JCS].
D.JCS_CODE		(A): Added from [PP-JCS].
D.JCS_DATA		(A): Added from [PP-JCS].
D.SEC_DATA		(A): Added from [PP-JCS].

Table 6. Assets Consistency table

3.4.2.2 Users and Subjects consistency

All Users defined in Base-PP [PP-eUICC] are relevant for the TOE of this Security Target. All users are described in section 4.2.

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	(D) : this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only.

Table 7. User consistency table

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

All subjects are described in section 4.2.

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

Subjects	PP-eUICC	Security Target
S.ISD-R	X	(R): this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only.
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].

Table 8. Subjects Consistency table

3.4.2.3 Threats consistency

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

All threats are described in section 4.3.

The table below indicates the Threats' consistency.

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. Additionally, this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only.
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	(R): this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only.
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)
T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)

Table 9. Threats Consistency table

3.4.2.4 Organizational Security Policies consistency

All Organizational Security Policies defined in [PP-eUICC] are relevant for the TOE of this Security Target. All OSPs are described in section 4.4.

The table below indicates the Organizational Security Policies' consistency.

OSPs	PP-eUICC	Security Target
OSP.LIFE-CYCLE	X	(R): this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only

Table 10. Organizational Security Policies Consistency table

3.4.2.5 Assumptions consistency

All Assumptions defined in [PP-eUICC] are relevant for the TOE of this Security Target. All assumptions are described in section 4.5.

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

Assumptions	PP-eUICC	Security Target

A.TRUSTED-PATHS-LPAd-IPAd	X	(R): this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.CAP_FILE		(A): Added from [PP-JCS]
A.Process-Sec-IC		(A): Added from [PP-0084]

Table 11. Assumptions Consistency table

3.4.3 Security Objectives Consistency

3.4.3.1 Objective for the TOE consistency

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

All objectives are described in section 5.

The table below indicates the Security Objectives' consistency.

Note that OE.RE* and OE.IC* from [PP-eUICC] become security objectives from 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.PRE-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		(A) Replaces OE.IC.PROOF_OF_IDENTITY from PP-eUICC
O.IC.SUPPORT		(A) Replaces OE.IC. SUPPORT from PP-eUICC

O.IC.RECOVERY		(A) Replaces OE.IC. RECOVERY from PP-eUICC
O.RE.PRE-PPI		(A) Replaces OE.RE.PRE-PPI from PP-eUICC
O.RE.SECURE-COMM		(A) Replaces OE.RE.SECURE-COMM from PP-eUICC
O.RE.API		(A) Replaces OE.RE.API from PP-eUICC
O.RE.DATA-CONFIDENTIALITY		(A) Replaces OE.RE.DATA-CONFIDENTIALITY from PP-eUICC
O.RE.DATA-INTEGRITY		(A) Replaces OE.RE.DATA-INTEGRITY from PP-eUICC
O.RE.IDENTITY		(A) Replaces OE.RE.IDENTITY from PP-eUICC
O.RE.CODE-EXE		(A) Replaces OE.RE.CODE-EXE from PP-eUICC

Table 12. Security objectives for the TOE consistency table

3.4.3.2 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	(R): this TOE implements GSMA eSIM IoT Architecture and Requirements for IoT Devices only
OE.APPLICATIONS	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.MNO-SD	X	(E)
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-CONFIDENTIALITY	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.Process-Sec-IC		(A): Added from [PP-0084]

Table 13. Security objectives for the Operational Environment consistency table

3.4.4 Conformity of the Requirement (SFR/SAR)

3.4.4.1 SFR consistency

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	Assignment performed.
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. Refined.
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)
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/Base	X	(E)
FCS_COP.1/Mobile_network	X	Selection 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].
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		(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** **/SIG_ECC** **/ECDH** **/MAC_TDES** **/MAC_AES** **/HMAC** **/CIPH_TDES** **/CIPH_AES** **/CIPH_AES_GCM** **/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].
FCS_CKM.1/GP-SCP		(A): Added from [PP-GP]
FCS_COP.1/GP-SCP		(A): Added from [PP-GP]
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].
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.RECOVERY.
FPT_RCV.4		(A): Added to cover O.IC.SUPPORT.
FPT_PHP.3		(A): Added to cover O.IC.SUPPORT.
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]. Refinement of FDP_UIT.1/CM
FDP_UCT.1/GP		(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]. Refinement of FDP_IFC.2/CM

FMT_MSA.3/GP		(A): Added from [PP-GP]. Refinement of FMT_MSA.3/CM
FMT_MSA.1/GP		(A): Added from [PP-GP]. Refinement of FMT_MSA.1/CM
FMT_SMR.1/GP		(A): Added from [PP-GP]. Refinement of FMT_SMR.1/Installer and FMT_SMR.1/CM.
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]. Refinement of FTP_ITC.1/CM
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP]. Refinement of FDP_IFF.1/CM
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]. Refinement of FIA_UID.1/CM
FPT_TDC.1/GP		(A): Added from [PP-GP]
FCO_NRO.2/GP		(A): Added from [PP-GP]. Refinement of FCO_NRO.2/CM
FDP_ROL.1/GP		(A): Added from [PP-GP]

Table 14 Security Functional Requirement consistency table

3.4.4.2 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.

4. Security Problem definition

This chapter introduces the security problem addressed by the TOE and its operational environment. The security problem consists of the threats the 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.

4.1 Assets

The definition of the assets from [PP-eUICC] and [PP-JCS] is not repeated here.

See section 3.4.2.1 for complete list of assets.

4.2 Users and Subjects

The definition of users and subjects from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here.

See section 3.4.2.2 for a complete list of users and subjects.

The Refined subject description is detailed below:

S.ISD-R

The ISD-R is responsible for the creation of new ISD-Ps and life-cycle management of all ISD-Ps.

The ISD-R includes IPA that provides the necessary access to the services and data required by IPA functions. IPA Services are mandatory, regardless of the fact whether it is IPAe which is active.

The ISD-R acts also as an object. In this case, it is named SO.ISD-R.

4.3 Threats

The definition of threats from [PP-eUICC] where no refinements are made is not repeated here.

See section 3.4.2.3 for complete list of threats.

Refined threats description are detailed below:

T.UNAUTHORIZED-PROFILE-MNG

The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.

Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.APP_C_DATA, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_CODE.

T.UNAUTHORIZED-PLATFORM-MNG

The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.

Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behaviour of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG

T.PROFILE-MNG-INTERCEPTION

The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.

Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P and ISD-R), D.PROFILE_*., D.APP_C_DATA, D.PIN and D.APP_KEYs.

T.PROFILE-MNG-ELIGIBILITY

An off-card or on-card actor alters or eavesdrops the transmission between eUICC and SM-DP+ (ES8+), or alters the Device Information when provided from the IPAd to the eUICC, in order to compromise the eligibility of the eUICC, for example:

- downgrade the security of the profile sent to the eUICC by claiming compliance to a previous version of the specification, or lack of cryptographic support;
- to obtain an unauthorized profile by modifying the Device Info or eUICC identifier.

NOTE: the attacker may be an on-card application intercepting transmissions to the security domains, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device

Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, D.APP_C_DATA, D.PIN, D.APP_KEYs, D.APP_CODE and D.APP_I_DATA.

T.UNAUTHORIZED-IDENTITY-MNG

The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.

Directly threatens the assets: 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, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA.

T.IDENTITY-INTERCEPTION

The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.

Directly threatens the assets: D.SECRETS, D.EID, D.APP_C_DATA, D.PIN and D.APP_KEYs.

T.LPAd-INTERFACE-EXPLOIT

An off-card actor exploits the interfaces to IPAd (interfaces ES10a and ES10b) to:

- either impersonate the IPAd (Man-in-the-middle, masquerade), or
- exploit a flaw in the interface to modify or disclose sensitive assets, or execute code (extension of T.LOGICAL-ATTACK and T.PHYSICAL-ATTACK targeting specifically the interfaces to IPAd).

The attacker could thus perform unauthorised profile and platform management, execute eUICCMemoryReset (SGP.32), or Add Initial eIM (SGP.32).

The attacker could also compromise the eligibility check process by compromising the Device Information that is normally passed on from the IPAd to the eUICC before profile download and installation.

The difference to the threats T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, and T.PROFILE-MNG-ELIGIBILITY, is on the interfaces used to perform the attack (ES10a,b).

Directly threatened asset: D.DEVICE_INFO, D.PLATFORM_DATA.

T.LOGICAL-ATTACK

The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.

Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, D.JCS_CODE, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_C_DATA..

4.4 Organizational Security Policies

See section 3.4.2.4 for complete list of organizational security policies.

The Refined OSP description is detailed below:

OSP.LIFE-CYCLE

The TOE must enforce the eUICC life-cycle defined in [SGP.22]. In particular:

- There is a limit on the number of ISD-Ps enabled at a time.
- The eUICC must enforce the profile policy rules (PPR) in case a profile state change is attempted (installation, disabling or deletion of a profile), except during the memory reset or test memory reset functions: in this case, the eUICC may disable and delete the currently enabled profile, even if a PPR states that the profile cannot be disabled or deleted;
- The eUICC must enforce the rules authorisation table (RAT) before a profile containing PPRs is authorised to be installed on the eUICC

4.5 Assumptions

The definition of assumptions from [PP-eUICC], [PP-0084] and [PP-JCS] where no refinements are made is not repeated here.

See section 3.4.2.5 for complete list of organizational security policies.

The Refined subject description is detailed below:

A.TRUSTED-PATHS-LPAd-IPAd

It is assumed that the interfaces ES10a and ES10b are trusted paths between the eUICC and IPAd, when IPAd is present and active. It is also assumed that the IPAd is a trusted component.

It is assumed thatIPAd is protected against misuse.

It is assumed that the Device manufacturer is securing the following operations (SGP.32):

- Add of an initial eIM Configuration Data by the IPA.
- Complete removal of eIM Configuration Data by the IPA.

5. Security Objectives

This section introduces the security objectives for the TOE.

5.1 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 3.4.3 for complete list of 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 3.4.3.2 and their description are listed next:

Sec. 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: load of a package file, 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, 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.

Table 15. Security Objectives TOE

5.2 Security Objectives for the Operational Environment

The list and definitions of the security objectives for the operational environment from [PP-eUICC], [PP-0084] and [PP-JCS] where no refinements are made is not repeated here.

See section 3.4.3.2 for complete list of Security Objectives for the Operational Environment.

The Refined security objective for the operational environment description is detailed below:

OE.TRUSTED-PATHS-LPAd-IPAd

The interfaces ES10a and ES10b are trusted paths between the eUICC and IPAd, when IPAd is present and active. IPAd are trusted components and IPAd are protected against misuse. The Device manufacturer is securing the following operations:

- Add of an initial eIM Configuration Data by the IPA.
- Complete removal of eIM Configuration Data by the IPA.

5.3 Security Objectives Rationale

5.3.1 Threats

5.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

This threat is covered by requiring authentication and authorization from the legitimate actors:

- O.PRE-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.PRE-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.

5.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

O.PRE-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 eSIM CA will manage securely its credentials off-card.

5.3.1.3 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).

5.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

OE.TRUSTED-PATHS-LPAd-IPAd ensures that the interfaces ES10a and ES10b are trusted paths to the IPA.

5.3.1.5 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.

5.3.1.6 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, PRE 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.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY). However these sensitive data are also processed by the PRE, PPI and the Telecom Framework, which are not protected by these mechanisms. Consequently,

- the TOE itself must ensure the correct operation of PRE, PPI and Telecom Framework (O.OPERATE), and

- PRE, 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).

5.3.2 Organizational Security Policies

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

5.3.3 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. A.Process-Sec-IC is defined as in [PP-0084] section 4.4.

5.3.4 Rationale Tables

5.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PRE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Section 5.3.1.1
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, OE.APPLICATIONS, OE.SM-DP+, OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.EIM (SGP.32)	Section 5.3.1.1
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 5.3.1.1
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 5.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 5.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 5.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.OPERATE, O.RE.API,	Section 5.3.1.6

	O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 5.3.1.6

Table 16. Threats and Security Objectives-Coverage

Security Objectives	Threats
O.PRE-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.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.SM-DS	
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.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.UNAUTHORIZED-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
OE.CAP_FILE	
OE.Process-Sec-IC	

Table 17. Security Objectives and threats

5.3.4.2 Organizational Security Policies Rationale

Organizational Security Policies	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PRE-PPI, OE.RE.PRE-PPI, O.OPERATE	Section 5.3.2

Table 18. Organizational Security Policies and Security Objectives-Coverage

Security Objectives	Organizational Security Policies
O.PRE-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.SM-DS	
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.CODE-EVIDENCE	
OE.MNO-SD	
OE.CAP_FILE	
OE.Process-Sec-IC	

Table 19. Security Objectives and Organizational Security Policies

5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.3
A.ACTORS	OE.CI, OE.SM-DP+, OE.MNO, OE.EIM (SGP.32), OE.SM-DS	Section 5.3.3

A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	Section 5.3.3
A.CAP_FILE	OE.CAP-FILE	Section 5.3.3
A.Process-Sec-IC	OE.Process-Sec-IC	Section 5.3.3

Table 20. 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.EIM (SGP.32)	A.ACTORS
OE.TRUSTED-PATHS-LPAd-IPAd	A.TRUSTED-PATHS-LPAd-IPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.MNO-SD	
OE.CAP_FILE	A.CAP-FILE
OE.Process-Sec-IC	A.Process-Sec-IC

Table 21. Assumptions and Security Objectives for the Operational Environment

6. 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.

7. Security Functional 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 3.4.4.1 added for secure RE support.
FPT_PHP.3, FPT_RCV.3, FPT_RCV.4 and FAU_SAS.1	Added for secure IC support.
[PP-GP] SFRs	Added for Card Content Management.

Table 22 SFRs of the TOE of this ST

7.1 eUICC Security Functional Requirements

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

7.1.1 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: *No additional TSF mediated actions*]**[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.

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**

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

- **[assignment: *No additional TSF mediated actions*][2]**

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

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 1:

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.32]:

- *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*][3].**

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

[3] [selection: eIM ID is associated to S.ISD-R, acting on behalf of U.EIM, no other associations]

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)*][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;**
- **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*][5]**.**

Application note 2 :

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+**

[4] [selection: Initial association of eIM ID requires U.EIM to be authenticated via CERT.EIM.ECDSA (SGP.32), no other initial associations]

[5] [selection: change of eIM ID requires U.EIM to be authenticated via "CERT.EIM.ECDSA (SGP.32), no other changes]

- **U.MNO-OTA**
- **[Selection: *U.EIM (SGP.32)*]**[6]

Application note 3:

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 4:

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.

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+;**

[6] [Selection: none, U.EIM (SGP.32)]

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

- **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*]**[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.

7.1.2 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:

- **users/subjects:**
  - **U.SM-DP+, SO.ISD-P and S.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.MNOSD 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].

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

[9] [assignment: additional information flow control SFP rules]

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**.

FTP_ITC.1/SCP Inter-TSF trusted channel

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 5:

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. The requirements stated by [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.32], sections 2.6 and 5.5.*
- *SCP80 must be provided to build secure channels to MNO OTA Platform (section 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.*

Related keys are:

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

[10] [assignment: rules, based on security attributes, that explicitly authorise information flows]

[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 IPAd to transmit the following operations:*
    - *ES10a.GetEuiccConfiguredAddresses*
    - *ES10b.SetDefaultDpAddress (SGP.32)*
    - *ES10b.PrepareDownload*
    - *ES10b.LoadBoundProfilePackage*
    - *ES10b.GetEUICCChallenge*
    - *ES10b.GetEUICCInfo*
    - *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)*
    - *ES10b.GetEID (SGP.32)*
    - *ES10b.GetRAT*
  - *The TSF may permit the IPAd to transmit the following operations:*
    - *ES10b.eUICCMemoryReset (SGP.32)*
    - *ES10b.ExecuteFallbackMechanism (SGP.32)*
    - *ES10b.ReturnFromFallback (SGP.32)*
    - *ES10b.EnableEmergencyProfile (SGP.32)*
    - *ES10b.DisableEmergencyProfile (SGP.32)*
    - *ES10b.GetConnectivityParameters (SGP.32)*

- *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.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] §5.8-5.9-5.13 IPAd command]***[13]

when interpreting the TSF data from another trusted IT product.

[12] [assignment: additional importation control rules]

13 [assignment: list of interpretation rules to be applied by the TSF]

Application note 6:

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*
- *IPAd commands*
  - *ES10a.GetEuiccConfiguredAddresses*
  - *ES10b.SetDefaultDpAddress (SGP.32)*
  - *ES10b.PrepareDownload*
  - *ES10b.LoadBoundProfilePackage*
  - *ES10b.GetEUICCChallenge*
  - *ES10b.GetEUICCInfo*
  - *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)*
  - *ES10b.eUICCMemoryReset (SGP.32)*
  - *ES10b.GetEID (SGP.32)*
  - *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 integrity

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].

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]***[15] that meets the following: **[assignment: *[GP] §11.8 §11.11, [SGP.32] §5.9.8*]**[16].

Application note 7:

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 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].

14 [assignment: at least one elliptic curve referenced in SGP.22 [24] or SGP.32 [36]]

15 [assignment: cryptographic key distribution method]

16 [assignment: list of standards]

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

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]**.**

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-MNO in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values*]**[21] that meets the following: **[assignment: *none*]**[22].

7.1.3 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:**
  - **S.ISD-P with security attributes "state" "PPR", and [Selection: *no additional attributes*]**[23]
- **operations:**
  - **Create and configure profile**
  - **Store profile metadata**
  - **Enable profile**
  - **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:**

---

[18] [assignment: cryptographic key destruction method]

[19] [assignment: list of standards]

[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]

- **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].

Application note 8:

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.32]:

- *ES8+.ConfigureISDP (Create and configure profile)*
- *ES8+.StoreMetadata (Store profile metadata)*
- *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)*
- *ESep.Disable (Disable Profile)*
- *ESep.Delete (Delete Profile)*

FDP_ACC.1/ECASD Subset access control

[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]

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: *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, CERT.DP.TLS, CERT.DSauth.ECDSA, or CERT.DS.TLS, provided by an ISD-R, with the CI public key (PK.CI.ECDSA)**
  - **Creation of an eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R**.
- **[assignment: *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].

---

[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]

[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]

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

7.1.4 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

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**

[31] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

[32] [selection: no additional operations]

- **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**.

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**

[33] [selection: 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]

[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]

- **[selection: *no additional functions*]**[38]

- **[assignment: *none*]**[39]**.**

7.1.5 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:**

(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 9:

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 TSF 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

[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]

[41] [assignment: list of security capabilities]

[42] [selection: bits, octets of bits, numbers [assignment: format of the numbers]]

[43] [assignment: a defined quality metric of the selected RNG class]

1	**[assignment: *information about IC power consumption, electromagnetic radiation, radio emission, internal state transition and timing during command execution*]**[44]	Any	-	• D.SECRETS; • D.SK.EUICC.ECDSA and the secret keys which are part of the following keysets: • D.MNO_KEYS, • D.PROFILE_NAA_PARAMS.

Application note 10:

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/Base	**Stored data integrity monitoring**

FDP_SDI.1.1/Base The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **integrity-sensitive data**.

Refinement:

The notion of integrity-sensitive data covers the following assets of the TOE:

- D.MNO_KEYS
- Profile data
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE _RULES
- Management data
  - D.PLATFORM_DATA
  - D.DEVICE_INFO

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

- D.PLATFORM_RAT
- Identity management data
  - D.SK.EUICC.ECDSA
  - D.CERT.EUICC.ECDSA
  - D.PK.CI.ECDSA
  - D.PK.EIM.ECDSA (SGP.32)
  - D.EID
  - D.SECRETS
  - D.CERT.EUM.ECDSA
  - D.CRLs if existing

FDP_RIP.1/Base Subset residual information protection

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 **Security Channel protocol information flow SFP, ISD-P content access control SFP and ISD-R access control SFP** to restrict the ability to change_default, query, modify and delete the security attributes

- D.PROFILE_RULES

To

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

FMT_MSA.1/CERT_KEYS Management of 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)]

FMT_MSA.1.1/CERT_KEYS The TSF shall enforce the **Security Channel protocol information flow SFP, ISD-R access control SFP and ECASD access control SFP** to restrict the ability to query and delete the security attributes

- **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: *"ESep.Delete" (SGP.32)*]**[46]
- **no actor for other operations.**

Application note 11:

The modification of D.MNO_KEYS keysets is forbidden. To modify the key-sets, 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.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**
  - **S.ISD-P**

[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.ECASD**
- **S.PPI**
- **S.PRE**
- **S.TELECOM**

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

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/Base	Static attribute initialisation

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

7.1.6 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, [selection: *no other algorithm*]**[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: *no additional standards*]**[50]

[49] [selection: *[assignment: cryptographic algorithms], no other algorithm*]

[50] [selection: *[assignment: list of standards], no additional standards*]

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*]**[51] that meets the following: **[assignment: *[SGP.32] §3.2, §5.9.8, [SIMalliance] §8.6.3]***[52].

FCS_CKM.6/Mobile_network Cryptographic key destruction

FCS_CKM.6.1/Mobile_network The TSF shall destroy **MILENAGE keys, TUAK keys and [selection: *no other keys of the cryptographic algorithm*]** [53]when **[selection: *no longer needed*]**[54].

FCS_CKM.6.2/Mobile_network The TSF 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]***[55] that meets the following: **[assignment: *none]***[56].

7.2 Runtime Environment Security Requirements

In [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 3.4.3.1). They subsequently have to be covered by SFRs that have been imported here from [PP-JCS] (as shown in section 3.4.4.1).

The Subjects (prefixed with an "S"), the Objects (prefixed with an "O"), Information (prefixed with an "I") are defined and described in [PP-JCS] section 7.2. Security attributes linked to these subjects, objects and information are also defined in [PP-JCS] section 7.2. Finally, Operations (prefixed with "OP") definition and description are present in [PP-JCS] section 7.2.

7.2.1 Core_LG Security Functional requirements

7.2.1.1 Firewall Policy

[51] [assignment: *cryptographic key distribution method*]

[52] [assignment: *list of standards*]

[53] [selection: [assignment: *keys of the cryptographic algorithms], no other keys of the cryptographic algorithm]*]

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

[55] [assignment: *cryptographic key destruction method*]

[56] [assignment: *list of standards*]

FDP_ACC.2/FIREWALL Complete access control

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

FDP_ACF.1/FIREWALL Security attribute based access control

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

FDP_IFC.1/JCVM Subset information flow control

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

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes
S.JCVM	Currently Active Context

Table 23. FDP_IFF.1/JCVM Simple security attributes

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

- **An operation OP.PUT(S1, S.MEMBER, I.DATA) is allowed if and only if the Currently Active Context is "Java Card RE";**
- **other OP.PUT operations are allowed regardless of the Currently Active Context's value**.

FDP_IFF.1.3/JCVM The TSF shall enforce the **[assignment: *none*]**[57].

FDP_IFF.1.4/JCVM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[58].

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **[assignment: *none*]**[59].

FDP_RIP.1/OBJECTS Subset residual information protection

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

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

FMT_MSA.1/JCRE Management of security attributes

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

FMT_MSA.1/JCVM Management of security attributes

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

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

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

FMT_MSA.3/FIREWALL Static attribute initialisation

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

FMT_MSA.3/JCVM Static attribute initialisation

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

FMT_SMF.1/RE Specification of Management Functions

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

FMT_SMR.1/RE Security roles

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

7.2.1.2 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 in Table 24*]** [60]and specified

[60] [assignment: cryptographic key generation algorithm]

cryptographic key sizes **[assignment: *cryptographic key sizes in Table 24*]**[61] that meet the following: **[assignment: *list of standards in Table 24*]**[62]

Iteration	Cryptographic key generation algorithm	Cryptographic key sizes	List of standards
/ECC	**G+D EC key generator**	**NIST P-256, curve25519**	**[RFC5639] chapter 3, [RFC8032]**

Table 24. List of cryptographic key generation algorithms for assignments 60 61 62

FCS_CKM.6/RE Cryptographic key destruction

FCS_CKM.6.1/RE The TSF shall destroy **[assignment: *ECC keys, Triple DES keys, AES keys*]**[63] when **[selection: *no longer needed*]**[64].

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*]**[65] that meets the following: **[assignment: *none*]**[66].

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform ***[assignment: cryptographic operations in Table 25]***[67] in accordance with a specified cryptographic algorithm ***[assignment: in Table 25]***[68] and cryptographic key sizes ***[assignment: in Table 25]***[69] that meet the following: ***[assignment: list of standards Table 25]***[70]

[61] [assignment: cryptographic key sizes]

[62] [assignment: list of standards]

[63] [assignment: list of cryptographic keys (including key material)]

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

[65] [assignment: cryptographic key destruction method]

[66] [assignment: list of standards]

[67] [assignment: list of cryptographic operations]

[68] [assignment: cryptographic algorithm]

[69] [assignment: cryptographic key sizes]

[70] [assignment: list of standards]

Iteration	Operation	Algorithm	Key sizes	List of standards
/SHA	hashing	SHA-1 SHA-224, 256, 384, 512	n.a.	[FIPS180-4]
/SIG_ECC	digital signature generation and verification	ECDSA	256	[FIPS186-4] [BSI TR 03111] [RFC5639]
/ECDH	key agreement	ECDH	256 bits	[SP800-56A] [RFC7748]
/MAC_TDES	MAC or HMAC generation and verification	Triple-DES CBC MAC	112, 168 bits	[FIPS46-3], Chapter 'TRIPLE DATA ENCRYPTION ALGORITHM', [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
/HMAC		With SHA-1, SHA-256, 384, 512	n.a.	[FIPS198-1] [RFC2104]
/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 25. List of cryptographic operations for assignments 67 68 69 70

Application note 12:

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-DPplus 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 de-fined 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.*

FDP_RIP.1/ABORT Subset residual information protection

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

FDP_RIP.1/APDU Subset residual information protection

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

FDP_RIP.1/bArray Subset residual information protection

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

FDP_RIP.1/GlobalArray Subset residual information protection

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

FDP_RIP.1/KEYS Subset residual information protection

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

FDP_RIP.1/TRANSIENT Subset residual information protection

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

FDP_ROL.1/FIREWALL Basic rollback

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

FCS_CKM.1/GP-SCP Cryptographic key generation

FCS_CKM.1.1/GP-SCP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: *cryptographic key generation algorithm in Table 26*]**[71] and specified cryptographic key sizes **[assignment: *cryptographic key sizes in Table 26*]**[72] that meet the following: **[assignment: *list of standards in Table 26*]**[73]**.**

SCP Protocol	Cryptographic key generation algorithm	Cryptographic key sizes	List of standards
SCP80	AES, TDES	TDES: 112 bits AES: 128, 192, or 256 bits	[TS 102 225]
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		[GP AM B]
SCP02	TDES	112 bits	[GP] section E.4.1
SCP03	AES	128, 192, or 256 bits	[GP AM D] section 6.2.1

Table 26 Cryptographic Key Generation Algorithms for assignments 71 72 73

FCS_COP.1/GP-SCP Cryptographic operation

[71] [assignment: cryptographic key generation algorithm]
[72] [assignment: cryptographic key sizes]
[73] [assignment: list of standards]

FCS_COP.1/GP-SCP The TSF shall perform **[assignment: *list of cryptographic operations in Table 27*]**[74] in accordance with a specified cryptographic algorithm **[assignment: *cryptographic algorithm in Table 27*]**[75] and cryptographic key sizes **[assignment: *cryptographic key sizes in Table 27*]**[76] that meet the following: **[assignment: l*ist of standards in Table 27*]**[77].

SCP protocol	Cryptographic Operations	Cryptographic Algorithm	Cryptographic Key Sizes	List of Standards
SCP02	MAC Generation/ Verification	H-MAC, CMAC using TDES	112 bits	[FIPS 198]
SCP02	Symmetric Encryption/ Decryption	TDES in CBC mode	112 bits	[NIST 800-67], [NIST 800-38A]
SCP02	Key Derivation	HMAC-based KDF, CMAC-based KDF using TDES	112 bits	[NIST 800-108], [FIPS 198]
SCP03	Symmetric Encryption/ Decryption	AES in CBC mode	128, 192, or 256 bits	[FIPS 197], [NIST 800-38A] and [FIPS 140-2]
SCP03	MAC Generation/ Verification	CMAC AES	128, 192, or 256 bits	[NIST 800-38B] and [FIPS 140-2]
SCP03	Key Derivation	CMAC-based KDF using AES	128, 192, or 256 bits	[NIST 800-108], [NIST 800-38B]
SCP02, SCP03	Hash Computing	SHA-256, SHA-384, SHA-512		[ISO-10118-3] and [FIPS-180-4]
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 112 bits AES: 128, 192, or 256 bits	[TS 102 225] [TS 102 226]
SCP81	Secure communication channel with the Remote	TLS 1.2 with recommended cipher suites: TLS_PSK_WITH_AES_128_CBC_SHA256 TLS_PSK_WITH_NULL_SHA256		[GP Am B] section 3.3.2

[74] [assignment: list of cryptographic operations]
[75] [assignment: cryptographic algorithm]
[76] [assignment: cryptographic key sizes]
[77] [assignment: list of standards]

	Administration Server	TLS 1.3 with recommended cipher suites: TLS_AES_128_CCM_SHA256 TLS_AES_128_GCM_SHA256		

Table 27 Cryptographic Operations for assignments 74 75 76 77

7.2.1.3 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: *Card Lock / Application Lock*]**[78] upon detection of a potential security violation.

Refinement:

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

- CAP file inconsistency,
- 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)]***[79]

Application note 13:

Bytecode verification is performed off-card.

FDP_SDI.2/DATA	Stored data integrity monitoring and action

[78] [assignment: list of other actions]

[79] [assignment: list of other runtime errors]

FDP_SDI.2.1/DATA The TSF shall monitor user data stored in containers controlled by the TSF for **[assignment: *integrity errors*]**[80] on all objects, based on the following attributes: **[assignment: *checksum integrity (complementary value, EDC) of cryptographic keys, PIN values and their associated attributes*]**[81].

FDP_SDI.2.2/DATA Upon detection of a data integrity error, the TSF shall **[assignment: *bring the card into a secure state*]**[82].

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **[assignment: *unauthorized users or subjects*]**[83] are unable to observe the operation **[assignment: *cryptographic operations and comparison operations*]** [84] on **[assignment: *key values, PIN values*]**[85] by **[assignment: *S.JCRE, S.Applet]***[86].

FPT_FLS.1/RE Failure with preservation of secure state

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

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

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **the CAP files, the bytecode and its data arguments** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 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*]**[87]

when interpreting the TSF data from another trusted IT product.

7.2.1.4 AID Management

FIA_ATD.1/AID User attribute definition

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

[80] [assignment: integrity errors]
[81] [assignment: user data attributes]
[82] [assignment: actions to be taken]
[83] [assignment: list of users and/or subjects]
[84] [assignment: list of operations]
[85] [assignment: list of objects]
[86] [assignment: list of protected users and/or subjects]
[87] [assignment: list of interpretation rules to be applied by the TSF]

FIA_UID.2/AID User identification before any action

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

FIA_USB.1/AID User-subject binding

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

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/FIREWALL*]**[88].

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 behalf of users: **[assignment: *rules defined in FMT_MSA.3/FIREWALL]***[89].

FMT_MTD.1/JCRE Management of TSF data

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

FMT_MTD.3/JCRE Secure TSF data

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

7.2.2 INSTG Security Functional requirements

The InstG SFRs are not included. They are replaced by the following SFRs from [PP GP] as defined in section 7.2.7:

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].

[88] [assignment: list of rules for the initial association of attributes]
[89] [assignment: list of rules for the changing of attributes]

7.2.3 ADELG Security Functional Requirements

This group consists of the SFRs related to the deletion of applets and/or packages, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime. Deletion is a critical operation and therefore requires specific treatment. This policy is better thought as a frame to be filled by ST implementers.

FDP_ACC.2/ADEL Complete access control

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

FDP_ACF.1/ADEL Security attribute based access control

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

FDP_RIP.1/ADEL Subset residual information protection

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

FMT_MSA.1/ADEL Management of security attributes

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

FMT_MSA.3/ADEL Static attribute initialisation

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

FMT_SMF.1/ADEL Specification of Management Functions

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

FMT_SMR.1/ADEL Security roles

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

FPT_FLS.1/ADEL Failure with preservation of secure state

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

7.2.4 RMIG Security Functional Requirements

The product does not support RMI features.

7.2.5 ODELG Security Functional Requirements

The following requirements concern the object deletion mechanism. This mechanism is triggered by the applet that owns the deleted objects by invoking a specific API method.

FDP_RIP.1/ODEL Subset residual information protection

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

FPT_FLS.1/ODEL Failure with preservation of secure state

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

7.2.6 CARG Security Functional Requirements

The CarG SFRs are not included. They are replaced by the following SFRs from [PP GP] as defined in section 7.2.7:

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

7.2.7 Card Content Management Security Functional requirements

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 to 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 7.2.2 and 7.2.5.

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **[selection: [assignment: *1*][90]]** [91] 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**.

FIA_UAU.1/GP Timing of authentication

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

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*]**[92] user data in a manner protected from **modification, deletion, insertion, replay** errors.

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

Application note 14 :

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**.

---

[90] [assignment: positive integer number]

[91] [selection: [assignment: positive integer number], an administrator con-figurable positive integer within [assignment: range of acceptable values]]

[92] [selection: transmit, receive]

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*]**[93] user data in a manner protected from unauthorised disclosure.

Application note 15:

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 16:

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

[93] [selection: transmit, receive]

- **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 17:

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: *authorized identified roles from FMT_MSA.1/GP SFR*]**[94] to specify alternative initial values to override the default values when an object or information is created.

Application note 18:

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

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

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***

[94] [assignment: authorised identified roles]

***operations listed in tables below: from Table 28 to Table 31*]**[95]**]**[96] the security attributes **[assignment: *listed in the tables below: from Table 28 to Table 31*]**[97] to **[assignment: *the authorized identified roles listed in the tables below: from Table 28 to Table 31*]**[98].

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

[95] [assignment: other operations]

[96] [selection: change_default, query, modify, delete, [assignment: other operations]]

[97] [assignment: list of security attributes]

[98] [assignment: the authorised identified roles]

Table 28 GlobalPlatform Common Operations, Security Attributes, and Roles

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

Table 29 SCP02 Operations, Security Attributes, and Roles

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

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 30 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 31 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 19:

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 20:

This SFR corresponds to FMT_SMR.1/Installer and FMT_SMR.1/CM of [PP-JCS], 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*][99].**

FTP_ITC.1/GP Inter-TSF trusted channel

[99] [assignment: additional importation control rules]

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

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

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

- **APDU commands sent to the card within a Secure Channel Session**
- **When loading/installing a new ELF on the card**
- **When transmitting and loading sensitive data to the card using STORE DATA or PUT KEY commands**
- **When deleting ELFs, Applications, or Keys**
- **[assignment:**
  - ***When retrieving status information via GET STATUS Command***
  - ***When modifying the Application Life Cycle State via SET STATUS command*]**[100]**.

Application note 21:

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*]**[101] 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.

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

[101] [assignment: *list of information types*]

FCO_NRO.2.2/GP The TSF shall be able to relate the **[assignment: *identity*]**[102] of the originator of the information, and the **[assignment: *Executable Load Files, SD/Application data and keys*]**[103] of the information to which the evidence applies.

Refinement

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

FCO_NRO.2.3/GP The TSF shall provide a capability to verify the evidence of origin of information to **the off-card entity (recipient of the evidence of origin) who requested that verification given [assignment: *that the data origin authentication provided within the context of secure messaging was successful*]**[104].

Application note 22:

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*]**[105].

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

- **S. SD implements one or more Secure Channel Protocols, namely [selection: *SCP02, SCP03, SCP80, SCP81*]**[106]**, 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).**

---

[102] [assignment: *list of attributes*]

[103] [assignment: *list of information fields*]

[104] [assignment: *limitations on the evidence of origin*]

[105] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

[106] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]

- **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*][107].**

FDP_IFF.1.3/GP-ELF The TSF shall enforce the **[assignment: *none*]**[108].

FDP_IFF.1.4/GP-ELF The TSF shall explicitly authorise an information flow based on the following rules**: [assignment: *none*]**[109].

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

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- **S.OPEN fails to verify the Card Life Cycle state**
- **S.OPEN fails to verify the SD privileges.**
- **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.SD fails to unwrap INSTALL or LOAD commands.**
- **[assignment: *none*][110].**

Application note 23:

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.

---

[107] [assignment: for each operation, the security attribute-based re-lationship that must hold between subject and information secu-rity attributes]

[108] [assignment: additional information flow control SFP rules]

[109] [assignment: rules, based on security attributes, that explicitly author-ise information flows]

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

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.

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*][111].**

Application note 24:

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.

[111] [assignment: additional importation control rules]

FDP_IFF.1/GP-KL Complete information flow control

FDP_IFF.1.1/GP-KL The TSF shall enforce the **Data & Key Loading information flow control SFP** based on the following types of subject and information security attributes: **[assignment:**

- ***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*]**[112].

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, SCP80, SCP81*]**[113]**, each equipped with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application,**
- **S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the**
- **S.OPEN checks that the requesting S.SD has no restrictions for personalisation.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and prior to the command forwarding to the targeted Application or SD.**
- **[assignment: *none*]**[114]**.**

FDP_IFF.1.3/GP-KL The TSF shall enforce the **[assignment: *none*]**[115]**.**

FDP_IFF.1.4/GP-KL The TSF shall explicitly authorise an information flow based on the following rules**: [assignment: *none*]**[116]**.**

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

---

[112] [assignment: list of subjects and information controlled under the indi-cated SFP, and for each, the security attributes]

[113] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]

[114] [assignment: for each operation, the security attribute-based re-lationship that must hold between subject and information secu-rity attributes]

[115] [assignment: additional information flow control SFP rules]

[116] [assignment: rules, based on security attributes, that explicitly author-ise information flows]

- **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*][117].**

Application note 25:

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.
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 'AUTHENTI-CATED' 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 [Refined]	**Specification of Management Functions**

FMT_SMF.1.1/GP 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,~~**

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

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 26:

This SFR corresponds to FMT_SMF.1/CM of [PP-JCS], 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*][118] 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*]**[119] the TSF shall ensure the re-turn 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%*]**[120] 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 27:

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.

---

[118] [assignment: list of failures/service discontinuities during card content management operations]

[119] [assignment: list of failures/service discontinuities during card content management operations]

[120] [assignment: quantification]

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

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

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

FPT_FLS.1/GP Failure with preservation of secure state

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

- **S.OPEN fails to load/install an Executable Load File / Application instance.**
- **S.SD fails to load SD/Application data and keys.**
- **S.OPEN fails to verify/change the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **[assignment: *none*][121].**

Application note 18:

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.

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*]**[122] 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.

[121] [assignment: list of additional types of failures]

[122] [assignment: list of TSF-mediated actions]

Application note 28:

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*]**[123] 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*]**[124] when interpreting the TSF data from another trusted IT product.

7.2.8 Underlying platform IC Security Functional Requirements

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*]**[125] to the **[assignment: *TSF*]**[126] by responding automatically such that the SFRs are always enforced.

FAU_SAS.1 Audit Storage

[123] [assignment: list of TSF data types]

[124] [assignment: list of interpretation rules to be applied by the TSF]

[125] [assignment: physical manipulation and physical probing]

[126] [assignment: TSF]

FAU_SAS.1.1 The TSF shall provide **[assignment: *the test process before TOE Delivery*]**[127] with the capability to store **[assignment: *Initialisation Data]***[128] in the **[assignment: *NVM]***[129]**.**

FPT_RCV.3/OS Automated recovery without undue loss

FPT_RCV.3.1/OS When automated recovery from **[assignment: *none*]**[130]**,** 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*]**[131] 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*]**[132]

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 29

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

FPT_RCV.4 Function recovery

[127] [assignment: list of subjects]
[128] [assignment: list of audit information]
[129] [assignment: type of persistent memory]
[130] [assignment: list of failures/service discontinuities
[131] [assignment: list of failures/service discontinuities]]
[132] [assignment: quantification]

FPT_RCV.4.1 The TSF shall ensure that **[assignment: *reading from and writing to static and objects' fields interrupted by power loss*]**[133] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

7.3 Security Functional Requirements Rationale

7.3.1 SFRs for eUICC rationale

The security functional requirements rationale is the same than the ones present in section 6.3 from [PP-eUICC].

7.3.2 SFRs for Runtime Environment rationale

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 than the rationale for the objectives translated from JavaCard PP [PP-JCS] and are not repeated here.

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

RE objectives	Translation from JavaCard 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, OE.VERIFICATION
O.RE.API	O.CARD-MANAGEMENT, O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM, OE.VERIFICATION
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, OE.VERIFICATION

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

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.VERIFICATION

Table 32. Runtime environment objectives conversion for SFR rationale.

Note that 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.

7.3.3 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	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 33 IC Security Objectives and SFRs – Coverage

7.3.4 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], section 7.4.3.1.

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

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 Table 34. 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_COP.1 **/ECDH** **/MAC_TDES** **/MAC_AES** **/HMAC** **/CIPH_TDES** **/CIPH_AES** **/CIPH_AES_GCM** **/ECKA-EG**	(FCS_CKM.1, FCS_CKM.5, FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FCS_CKM.1 FCS_CKM.6
FPT_PHP.3	No Dependencies	No Dependencies
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4	No Dependencies	No Dependencies
FAU_SAS.1	No Dependencies	No Dependencies

Table 34 Extension of SFR Dependencies

7.3.4.1 Rationale for the exclusion of dependencies

- The dependency FCS_CKM.3 of FCS_COP.1, FCS_CKM.1 and FCS_CKM.2 is discarded. This dependency is discarded as there is no Interface to access the keys.

- The dependency FAU_SAA.1 of FAU_ARP.1 is discarded. The dependency of FAU_ARP.1 on FAU_SAA.1 assumes that a "potential security violation" generates an audit event. On the contrary, the events listed in FAU_ARP.1 are self-contained (arithmetic exception, ill-formed bytecodes, access failure) and ask for a straightforward reaction of the TSFs on their occurrence at runtime. The JCVM or other components of the TOE detect these events during their usual working order. Thus, there is no mandatory audit recording in this ST.

- The dependency of FCS_COP.1/SHA is discarded. This dependency is discarded as hash operation does not require any key.

- The dependency FIA_UID.1 of FMT_SMR.1/ADEL is discarded. This dependency is discarded as the identification of the "deletion manager" since it can be considered as part of the TSF.

- The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is discarded. This dependency is discarded as no management functions are required for the Java Card RE.

8. TOE Summary Specification

The TOE implements the SFRs in accordance to the GSMA specifications, sufficiently hardened to counter attackers at AVA_VAN.5 level.

The TOE is equipped with following Security Features to meet the security functional requirements.

8.1 eUICC security functions

8.1.1 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.

8.1.2 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

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), PPR (FMT_MSA.1/PPR), (FMT_MSA.1/RAT) and keys (FMT_MSA.1/CERT_KEYS) with re-strictive 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.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/GP and FPT_TDC.1.2/SCP when interpreting the TSF data from another trusted IT product.

8.1.3 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.

8.1.4 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 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.

8.1.5 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 up-date of an application or a Security Domain.

Content changes are permitted according to the privileges that have been as-signed 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.

8.1.6 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,

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

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, 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]**
SCP-SGP22	ECDSA 256 bits, AES-128
SCP80	Triple-DES and AES CBC MAC
SCP81	Use of TLS 1.2 cipher suites is recommended: 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.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.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 AM D]** 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 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.

8.1.7 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:

- Applications may use the Java Card API method Key.clearKey() for key destruction.
- 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 according to **[GP]** §11.8, **[SGP.32]** §5.9.8.

- Profile download and installation according to **[SGP.32]** §3.2, §5.9.8, **[SIMalliance]** §8.6.3.
- Java Card API set methods of javacard.security classes AESKey, DESKey, ECKey, ECPrivateKey, ECPublicKey.

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

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.
- Java Card API class javacard.security.MessageDigest with algorithm SHA (ALG_SHA, ALG_SHA_224/256/384/ 512).

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

- ECDSA is provided to applications via the Java Card API methods defined in the javacard.security.Signature class.
    - Java Card API ECDSA based signatures (ALG_ECDSA_SHA*) are provided with SHA-1, SHA-224/256/384/512.
- 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
- ECDH as required by the Java Card API class javacard.security.KeyAgreement ALG_EC_* (all EC DH excluding PACE) and ALG_XDH (using Montgomery Curves).

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) and the Java Card API class javacard.security.Signature (ALG_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 CMAC as required by the Java Card API class javacard.security.Signature (ALG_AES_CMAC_128).
- HMAC as required by the Java Card API class javacard.security.Signature (ALG_HMAC_SHA*) with SHA-1, SHA-256/384/512.
- 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 and ECB modes as required by FDP_IFF.1/SCP (SCP80/81, SCP-SGP.22), FDP_UCT.1/SCP, SCP03, and the Java Card API class javacardx.crypto.Cipher.

- AES in GCM mode as required by TLS v1.3.

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

8.1.8 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][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.

8.1.9 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).

8.2 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.

8.2.1 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
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	SF.SECURITY
FMT_MSA.1/PLATFORM_DATA	SF.ACCESS_CONTROL
FMT_MSA.1/RULES	SF.ACCESS_CONTROL
FMT_MSA.1/CERT_KEYS	SF.ACCESS_CONTROL
FMT_SMF.1	SF.ACCESS_CONTROL
FMT_SMR.1/Base	SF.ACCESS_CONTROL
FMT_MSA.1/RAT	SF.ACCESS_CONTROL
FMT_MSA.3/Base	SF.ACCESS_CONTROL
FCS_COP.1/Mobile_network	SF.CRYPTO
FCS_CKM.2/Mobile_network	SF.CRYPTO
FCS_CKM.6/Mobile_network	SF.CRYPTO

Table 35. eUICC SFRs coverage

8.2.2 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	SF.CRYPTO
FCS_CKM.6/RE	SF.CRYPTO
FCS_COP.1 **/SHA** **/SIG_ECC** **/ECDH** **/MAC_TDES** **/MAC_AES** **/HMAC** **/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
FCS_CKM.1/GP-SCP	SF.CRYPTO
FCS_COP.1/GP-SCP	SF.CRYPTO
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

Table 36 Runtime Environment SFRs coverage

8.2.3 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	SF.SECURITY

Table 37 Secure IC SFRs Coverage

8.2.4 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
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/Base
	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_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
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.1/GP FPT_FLS.1/ADEL FPT_FLS.1/ODEL FDP_RIP.1/ADEL FDP_RIP.1/ODEL FPT_PHP.3

	FPT_RCV.3/OS FPT_RCV.4
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
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.6/RE FCS_COP.1/SHA FCS_COP.1/SIG_ECC FCS_COP.1/ECDH FCS_COP.1/MAC_TDES FCS_COP.1/MAC_AES

	FCS_COP.1/HMAC FCS_COP.1/CIPH_TDES FCS_COP.1/CIPH_AES FCS_COP.1/CIPH_AES_GCM FCS_COP.1/ECKA-EG FCS_CKM.1/GP-SCP FCS_COP.1/GP-SCP
SF.RNG	FCS_RNG.1
SF.IDENTITY	FIA_API.1 FAU_SAS.1

Table 38 Association table of SFRs and TSS

9. 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 [CC-CEM].

9.1 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]	TOE Security Functionality	Relevant	Not relevant
7.1	SF_DPM: Device Phase Management	x	
7.2	SF_PS: Protection against Snooping	x	
7.3	SF_PMA: Protection against Modifying Attacks	x	
7.4	SF_PLA: Protection against Logical Attacks	x	
7.5	SF_CS : Cryptographic Support	x	

Table 39 Classification of Platform-TSFs

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

9.2 Matching statement

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

- Certified microcontroller SLM17ECB800B & SLC17ECB800B.
- 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.
- Cryptographic support based on asymmetric key algorithms (ECDSA) with up to 521 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.

9.3 Security Functional Requirements

9.3.1 Security Functional Requirements

IC SFRs are separated in the following groups as defined in [CC-CEM]:

• IP_SFR: *Irrelevant* base component-SFRs not being used by the composite-ST;

• RP_SFR-SERV: *relevant* base component-SFRs being used by the composite-ST to implement a security service with associated TSFI;

• RP_SFR-MECH: *relevant* base component-SFRs being used by the composite-ST because of their security properties providing protection against attacks to the TOE as a whole and being addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the base component.

Platform SFR	Relevance	Correspondence in Composite ST
FRU_FLT.2	RP_SFR-MECH	FPT_RCV.3
FPT_FLS.1	RP_SFR-MECH	FPT_FLS.1/*, FPT_RCV.3
FMT_LIM.1	IP_SFR	Not Relevant
FMT_LIM.2	IP_SFR	Not Relevant
FAU_SAS.1	RP_SFR-MECH	FAU_SAS.1
FDP_SDC.1	RP_SFR-MECH	FPT_PHP.3, FPT_EMS.1/*
FDP_SDI.2	RP_SFR-MECH	FDP_SDI.2/DATA.
FPT_PHP.3	RP_SFR-MECH	FPT_PHP.3, FPT_EMS.1/Base
FDP_ITT.1	RP_SFR-MECH	FDP_IFC.1/JCVM
FPT_ITT.1	RP_SFR-MECH	FDP_ACF.1/FIREWALL, FPT_EMS.1/*
FDP_IFC.1	RP_SFR-MECH	FDP_IFC.1/JCVM, FDP_IFC.2/GP, FDP_IFC.1/Platform_services, FPT_EMS.1/*
FCS_RNG.1	RP_SFR-MECH	FCS_RNG.1
FCS_COP.1/TDES	IP_SFR	Not Relevant
FCS_CKM.4/TDES	IP_SFR	Not Relevant
FCS_COP.1/AES	IP_SFR	Not Relevant
FCS_CKM.4/AES	IP_SFR	Not Relevant
FMT_LIM.1/Loader	IP_SFR	Not Relevant
FMT_LIM.2/Loader	IP_SFR	Not Relevant
FTP_ITC.1	IP_SFR	Not Relevant
FDP_UCT.1	IP_SFR	Not Relevant
FDP_UIT.1	IP_SFR	Not Relevant
FDP_ACC.1/Loader	IP_SFR	Not Relevant

FDP_ACF.1/Loader	IP_SFR	Not Relevant
FIA_API.1	IP_SFR	Not Relevant
FPT_TST.2	IP_SFR	Not Relevant
FDP_ACC.1	RP_SFR-MECH	FDP_ACC.2/FIREWALL, FDP_ACC.2/ADEL, FDP_ACC.1/ECASD, FDP_ACC.1/ISDR
FDP_ACF.1	RP_SFR-MECH	FDP_ACF.1/FIREWALL, FDP_ACF.1/ADEL, FDP_ACF.1/ECASD, FDP_ACF.1/ISDR
FMT_MSA.1	RP_SFR-MECH	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/PPR, FMT_MSA.1/PLATFORM_DATA
FMT_MSA.3	RP_SFR-MECH	FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MSA.3/ADEL, FMT_MSA.3/GP, FMT_MSA.3/Base,
FMT_SMF.1	RP_SFR-MECH	FMT_SMF.1, FMT_SMF.1/ADEL, FMT_SMF.1/CM

Table 40 Platform SFR classification

9.3.2 Security Assurance Requirements

The Composite-ST requires EAL 4 according to Common Criteria 2022 release 1 augmented by ALC_DVS.2 and AVA_VAN.5

The Platform-ST has been certified to EAL 5 according to Common Criteria 2022 Release 1 augmented by ALC_DVS.2 and AVA_VAN.5.

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

9.4 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:

- O.Leak-Inherent
- O.Phys-Probing
- O.Malfunction
- O.Phys-Manipulation
- O.Leak-Forced
- O.Abuse-Func

- O.Identification
- O.RND
- 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
O.Leak-Inherent	X		
O.Phys-Probing	X		
O.Malfunction	X	X	
O.Phys-Manipulation	X		
O.Leak-Forced	X		
O.Abuse-Func	X		
O.Identification	X		X
O.RND	X		
O.Mem-Access	X		

Table 41 Correspondence of Objectives in Composite ST

O.IC.RECOVERY matches to 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 O.Identification from the Platform-ST because it provides capability of the TOE to store Initialisation Data and/or Prepersonalisation 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:

- O.Cap_Avail_Loader, O.Ctrl_Auth_Loader: these objectives are not relevant because the Composite-TOE is delivered only with disabled Loading capability.
- O.Authentication: it is not relevant, since it is not available after TOE delivery.
- O.Prot_TSF_Confidentiality: it is not relevant because the Composite-TOE is delivered only with disabled Loading capability (irreversible operation) and not delivered as an open sample.
- O.AES and O.TDES: these objectives are not relevant for the TOE because IC's cryptographic library (SCL) is not used by the composite-TOE. IC's cryptographic coprocessor is used as a hardware accelerator for AES operations.

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

9.5 Security objectives for environment

IC OEs are separated in the following groups as defined in appendix 1.1 of [CC-CEM]:

- IrOE: The objectives for the environment being not relevant for the TOE.
- CfPOE: The objectives for the environment being fulfilled by the TOE automatically.
- SgOE: The remaining IC OE which shall be addressed by the current TOE.

Platform ST Sec. Obj. Env.	**Correspondence in Composite ST**	
	Relevance	Rationale
OE.Resp-Appl	CfPOE	This objective is covered by the ADV_IMP.1 activity of the TOE evaluation.
OE.Process-Sec-IC	CfPOE / SgOE	This objective is covered by the ALC_DVS.2 activity of the TOE evaluation: - CfPOE: until TOE delivery - SgOE: phases d and e
OE.Lim_Block_Loader	IrOE	The Composite-TOE is delivered only with disabled Loading capability
OE.Loader_Usage	IrOE	The Composite-TOE is delivered only with disabled Loading capability
OE.TOE_Auth	IrOE	The Composite-TOE is delivered only with disabled Loading capability
OE.Secure_Delivery	CfPOE	This objective is covered by the ALC_DVS.2 activity of the TOE evaluation

Table 42 Correspondence of Objectives for Environment in Composite ST

10. Definitions

10.1 Abbreviations

Term	Description
CC	Common Criteria
O.ENV	Objective for the environment
O.TOE	Objective for the TOE
ST	Security Target

11. References

[AGD_PRE] Preparative Procedures for Sm@rtSIM® Tabit800 Consumer/M2M SGP.32 (confidential document), Version 1.6, 23.07.2026

SubMan eUICC Production Specification for Sm@rtSIM® Tabit800 Consumer/M2M SGP.32 (Confidential Document), Version 1.4, 23.07.2026

[AGD_OPE] Sm@rtSIM® Tabit800 Consumer/M2M SGP.32 Personalization Guide (Confidential Document), Version 0.0.3, 09.06.2026

SubMan eUICC Production Specification for Sm@rtSIM® Tabit800 Consumer/M2M SGP.32 (Confidential Document), Version 1.4, 23.07.2026

Sm@rtSIM® Tabit800 Consumer/M2M SGP.32 API Support (Confidential Document), Version 0.2, 28.05.2026

[AGD_SEC] Security Guidance for Sm@rtSIM® Tabit800 Consumer/M2M SGP.32 (confidential document), Version 1.3, 01.07.2026

[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

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

[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.

[CC-CEM] Common Methodology for Information Technology Security Evaluation, CCMB-2022-11-006, version CC:2022 Revision 1, November 2022.

[CC-ERRATA] Common Methodology for Information Technology Security Evaluation, Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 15-10-2025

[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

[FIPS198-1] Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, July 2008

[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 v2.3 Amendment E – Security Upgrade for Card Content Management, Version 1.1, October 2016.

[GP AM F] GlobalPlatform Card Specification v2.3 Amendment F – Secure Channel Protocol '11', Version 1.2.1, July 2018.

[GP SG] GlobalPlatform Card Composition Model Security Guidelines for Basic Applications, Version 2.0, December 2014.

[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

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

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

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

[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.

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

[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

[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>.

[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

[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>.

[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>.

[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.31] eSIM IoT Architecture and Requirements, version 1.2, GMSA Association, 26 April 2024.

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

[SGP.33-1] SGP.33-1 eSIM IoT Test Specification for the eUICC, Version 1.2, 27 January 2025.

[SGP.22] RSP Technical Specification, GSM Association, Version 2.5, 26 May 2023.

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

[SIMalliance] 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.

[SP800-56a] National Institute of Standards and Technology, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-67, rev. 3, April 2018.

[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] Infineon Technologies AG, Security Target Lite IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h, IFX_CCI_0037h T31 and M31, 25 August 2025

12. List of figures

13. List of tables