Giesecke+Devrient

Security Target Lite Sm@rtSIM Polaris SGP.22

Giesecke+Devrient Mobile Security

PUBLIC

Table of Contents

Table of Contents 2

1. ST Introduction 6

1.1 Security Target Reference 6

1.2 TOE reference 6

1.3 TOE scope 6

1.3.1 Physical scope 6

1.3.2 Logical scope 7

1.4 TOE Overview 7

1.4.1 TOE Description 7

1.4.2 TOE type and usage 8

1.4.3 TOE life cycle 8

1.4.4 Non-TOE HW/SW/FW available to the TOE 10

2. Conformance Claims 11

2.1 CC conformance claims 11

2.2 PP claim 11

2.3 Package claim 11

2.4 Conformance Claim Rationale 11

2.4.1 Conformity of the TOE Type 12

2.4.2 This STs additions and refinements to the PP 12

2.4.3 SPD Consistency 13

3. Security Problem Definition 29

3.1 Assets....29
3.2 Users and Subjects....29
3.3 Threats....30
3.4 Organisational Security Policies....31
3.5 Assumptions....32
4. Security objectives....33
4.1 Security objectives for the TOE....33
4.2 Security objectives for the operational environment....33
4.3 Security Objectives Rationale....34
4.3.1 Threats....34
4.3.2 Rationale Tables....39
5. Extended Requirements....48
6. Security Requirements....49
6.1 eUICC Security Functional Requirements....50
6.1.1 Introduction....50
6.1.2 Identification and authentication....50
6.1.3 Communication....51
6.1.4 Security Domains....53
6.1.5 Platform Services....55
6.1.6 Security management....56
6.1.7 Mobile Network authentication....59
6.2 Java Card System SFRs....62
6.2.1 CoreG_LC Security Functional Requirements....62
6.2.2 InstG Security Functional Requirements....70

6.2.3 ADELG Security Functional Requirements....71
6.2.4 ODELG Security Functional Requirements....71
6.2.5 CarG Security Functional Requirements....71
6.3 Card Content Management SFRs....75
6.4 Secure IC Platform SFRs....75
6.5 ITL SFRs....76
6.5.1 Class FIA: Identification and Authentication....76
6.5.2 Class FDP: User Data Protection....77
6.5.3 Class FMT: Security Management....80
6.5.4 Class FPT: Protection of the TSF....81
6.5.5 Class FTP: Trusted Path/Channels....82
6.6 Security Requirements Dependencies....83
6.7 Security Funcitonal Requirements Rationale....85
6.7.1 SFRs for eUICC rationale....85
6.7.2 SFRs for Runtime Environment rationale....85
6.7.3 SFRs for Underlying platform IC rationale....87
6.7.4 SFRs for ITL rationale....88
7. TOE Summary Specification (ASE_TSS)....90
7.1 SF.TRANSACTION....90
7.2 SF.ACCESS_CONTROL....90
7.3 SF.INTEGRITY....92
7.4 SF.SECURITY....92
7.5 SF.PLATFORM_MANAGEMENT....94
7.6 SF.SECURE_CHANNEL....95
7.7 SF.CRYPTO....97

7.8 SF.RNG 99
7.9 SF.IDENTITY 99
7.10 TSS Rationale 99
7.10.1 eUICC SFRs coverage 100
7.10.2 Runtime Environment SFRs coverage 102
7.10.3 Secure IC SFRs coverage 105
7.10.4 ITL SFRs coverage 105
7.10.5 Association table of SFRs and TSS 106
8. Statement of Compatibility 111
8.1 Classification of the Platform TSFs 111
8.2 Matching statement 112
8.3 Security objectives 113
8.4 Security objectives for the environment 116
8.5 Security requirements 117
8.5.1 Security Functional Requirements 117
8.5.2 Security Assurance Requirements 120
9. References 121
List of tables 127

1. ST Introduction

1.1 Security Target Reference

Name	Security Target Lite Sm@rtSIM Polaris SGP.22
Version	Version 2.8 / 26 June 2024
Reference	GDM_Sm@rtSIM_Polaris_SGP.22_ASE
ST template reference	[SGP.17]

1.2 TOE reference

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

1.3 TOE scope

1.3.1 Physical scope

Category	Component	Version	Delivery form
HW	ST33K1M5C CC certificate: NSCIB-CC-2300056-01-CERT [IC_ST]	IC Version D	wafer and package
FW	ST33K platform firmware	FW Version 3.1.4	Binary in memory

SW	Sm@rtSIM NextGeneration Polaris	1.0	Binary in memory
DOC	Operative guidance	[AGD_OPE]	pdf file
DOC	Preparative guidance	[AGD_PRE]	pdf file
DOC	Security guidance	[AGD_SEC]	pdf file

1.3.2 Logical scope

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

1.4 TOE Overview

The TOE is the embedded UICC software that implements the GSMA Remote SIM Provisioning (RSP) Architecture for Consumer Devices ([SGP.21] and [SGP.22]). As Runtime Environment, the TOE uses Java Card version 3.1. A detailed TOE overview is given in chapter 1.2 of [PP-eUICC]. To enable to update an already installed embedded OS, the TOE contains the Image Trusted Loader (ITL) software.

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

1.4.1 TOE Description

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

- The complete TOE of the PP (the Application Layer and the Platform layer as shown in Figure 1);
- The secure IC platform and OS;
- The Runtime Environment (the Java Card System).

- The Image Trusted Loader (ITL) which is a module that enables a full Firmware or full Operating System update. This update can be performed both in the factory (Over The Wire) or in the field (Over The Air), when the previous OS is already installed.

1.4.2 TOE type and usage

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

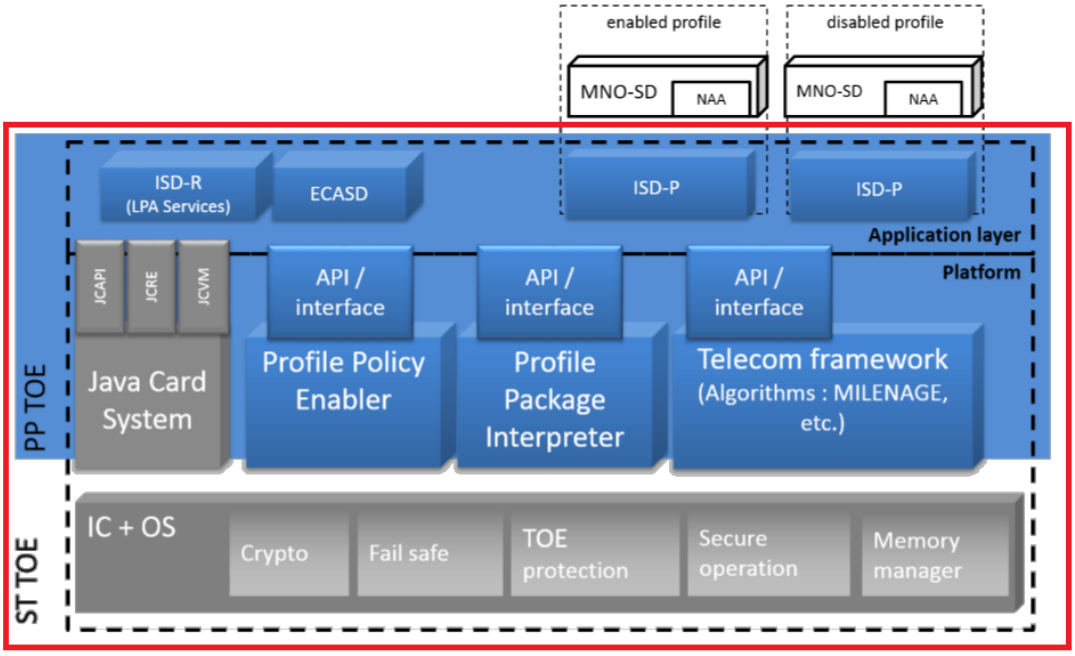

Figure 1 TOE Scope

1.4.3 TOE life cycle

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

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

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

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

Table 1 TOE life-cycle phases and TOE delivery

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

Non-TOE is same than the ones mentioned in the [PP-eUICC], except for IC and RE, which are in scope of the TOE.

The Profiles are not part of the TOE.

2. Conformance Claims

2.1 CC conformance claims

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

2.2 PP claim

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

2.3 Package claim

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

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

2.4 Conformance Claim Rationale

This Security Target is conformant to the claimed PP.

The TOE of this Security Target is the whole embedded UICC made of the IC, OS, RE and the TOE of the PP.

The objectives for the environment (that is for the IC, OS and RE) specified in the Protection Profile have become objectives for the TOE in this Security Target. These objectives have been partly fulfilled by a previous certificate (of an already certified IC) and partly translated in to SFRs.

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

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

The following notation used in the consistency tables in section 2.4.3:

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

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

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

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

2.4.1 Conformity of the TOE Type

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

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

2.4.2 This STs additions and refinements to the PP

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

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

The SFR FDP_SDI.1 from [PP-eUICC] was further refined to cover the asset D.TOE_IDENTIFIER.

Since the Runtime Environment is part of the TOE of this ST, SFRs defined in [PP-JCS] are included in this ST as indicated in2.4.3.8, Table 10.

The SFRs FTP_ITC.1/CCM are added to fulfill the secure card content management activities.

This ST includes additions related to the post-delivery loading of code (“in-the-field-loading”, abbreviated ITL) and secure personalization process.

2.4.3 SPD Consistency

2.4.3.1 Assets consistency

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

Assets	**PP-eUICC**	**Security Target**
D.MNO_KEYS	X	(E)
D.PRO-FILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_POL-ICY_RULES	X	(E)
D.PRO-FILE_USER_CODES	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)
D.EID	X	(E)

D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(E)
D.APP_C_DATA		(A) Added from [PP-JCS].
D.APP_I_DATA		(A) Added from [PP-JCS].
D.API_DATA		(A) Added from [PP-JCS].
D.JCS_DATA		(A) Added from [PP-JCS].
D.SEC_DATA		(A) Added from [PP-JCS].
D.APP_KEYs		(A) Added from [PP-JCS].
D.APP_CODE		(A) Added from [PP-JCS].
D.JCS_CODE		(A) Added from [PP-JCS].
D.CRYPTO		(A) Added from [PP-JCS].
D.UPDATE_IMAGE		(A)
D.TOE_IDENTIFIER		(A)

Table 2 Assets Consistency

2.4.3.2 Users and Subjects consistency

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

User	**PP-eUICC**	**Security Target**
U.SM-DPplus	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)

Table 3 Users consistency

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

Subjects	**PP-eUICC**	**Security Target**
S.ISD-R	X	(E)
S.ISD-P	X	(E)
S.ECASD	X	(E)
S.PPI	X	(E)
S.PPE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A) Added from [PP-JCS].
S.APPLET		(A) Added from [PP-JCS].
S.BCV		(A) Added from [PP-JCS].
S.CAD		(A) Added from [PP-JCS].
S.INSTALLER		(A) Added from [PP-JCS].
S.JCRE		(A) Added from [PP-JCS].
S.JCVM		(A) Added from [PP-JCS].
S.LOCAL		(A) Added from [PP-JCS].
S.MEMBER		(A) Added from [PP-JCS].
S.CAP_FILE		(A) Added from [PP-JCS].
S.SD		(A)
S.ITL		(A)

Table 4 Subjects Consistency

2.4.3.3 Threats consistency

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

Threats	**PP-eUICC**	**Security Target**
T.UNAUTHORIZED-PRO-FILE-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-PLAT-FORM-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-INTER-CEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-ELIGI-BILITY	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-IDEN-TITY-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.IDENTITY-INTERCEP-TION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-eUICC	X	(E)
T.LPAd-INTERFACE-EX-PLOIT	X	(E)
T.UNAUTHORIZED-MO-BILE-ACCESS	X	(E)

T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)
T.ITL.CONFID		(A)
T.ITL.UNAUTH		(A)
T.ITL.INTEG		(A)
T.ITL.INTERRUPT		(A)

Table 5 Threats Consistency

2.4.3.4 Organizational Security Policies consistency

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

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

Table 6 Organizational Security Policies Consistency

2.4.3.5 Assumptions consistency

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

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

Table 7 Assumptions Consistency

2.4.3.6 Objective for the TOE consistency

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

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

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

O.RE.API		Replaces OE.RE.API defined in PP-eUICC
O.RE.DATA-CONFIDENTIALITY		Replaces OE.RE.DATA-CONFIDENTIALITY defined in PP-eUICC
O.RE.DATA-INTEGRITY		Replaces OE.RE.DATA-INTEGRITY defined in PP-eUICC
O.RE.IDENTITY		Replaces OE.RE.IDENTITY defined in PP-eUICC
O.RE.CODE-EXE		Replaces OE.RE.CODE-EXE defined in PP-eUICC
O.ITL.SECURE_LOAD		(A)
O.ITL.CONFID_KEYS		(A)
O.TOE.IDENTIFICATION		(A)

Table 8 Security objectives for the TOE consistency

2.4.3.7 Objective for Environment consistency

O.ENV	**PP-eUICC**	**Security Target**
OE.CI	X	(E)
OE.SM-DPplus	X	(E)
OE.MNO	X	(E)
OE.TRUSTED-PATHS-LPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.CODE-EVIDENCE		(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.PPE-PPI	X	Removed and replaced by O.RE.PPE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTI-ALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIAL-ITY.
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.ITL.CONFID_IMAGE		(A) ST addition for post-issu-ance loading of updates.

Table 9 Security Objectives for the Operational Environment Consistency

2.4.3.8 SFR consistency

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

SFR	**PP-eUICC**	**Security Target**
FIA_UID.1/EXT	X	Assignment performed.
FIA_UAU.1/EXT	X	Assignment performed.
FIA_USB.1/EXT	X	(E)
FIA_UAU.4/EXT	X	(E)
FIA_UID.1/MNO-SD	X	Assignment performed.
FIA_USB.1/MNO-SD	X	(E)
FIA_ATD.1/eUICC	X	(R) Refined with iteration.
FIA_API.1/eUICC	X	(R) Refined with iteration.
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	(E)
FCS_CKM.2/SCP-MNO	X	Assignment performed.
FCS_CKM.4/SCP-SM	X	Assignment performed.
FCS_CKM.4/SCP-MNO	X	Assignment performed.

SFR	PP-eUICC	Security Target
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	Assignment performed.
FDP_ACC.1/ECASD	X	Assignment performed.
FDP_ACF.1/ECASD	X	Assignment performed.
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	Assignment performed.
FPT_FLS.1/Platform_services	X	Assignment performed.
FCS_RNG.1	X	Selection and assignment performed.
FPT_EMS.1/eUICC	X	(R) Refined with iteration. Assignment performed.
FDP_SDI.1/eUICC	X	(R) Refined with iteration. Covers an additional asset defined in this ST in the re-finement.
FDP_RIP.1/eUICC	X	(R) Refined with iteration.
FPT_FLS.1/eUICC	X	(R) Refined with iteration.
FMT_MSA.1/PLAT-FORM_DATA	X	(E)
FMT_MSA.1/PPR	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)

SFR	PP-eUICC	Security Target
FMT_SMF.1/eUICC	X	(R) Refined with iteration. Assignment performed.
FMT_SMR.1/eUICC	X	(R) Refined with iteration.
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3/eUICC	X	(R) Refined with iteration.
FCS_COP.1/Mobile_network	X	Selection performed.
FCS_CKM.2/Mobile_network	X	Assignment performed.
FCS_CKM.4/Mobile_network	X	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.

SFR	PP-eUICC	Security Target
FMT_SMR.1/RE		(A) Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/ECC, FCS_CKM.1/Triple DES, FCS_CKM.1/AES		(A) Added from [PP-JCS]. Refined with iteration.
FCS_CKM.4/RE		(A) Added from [PP-JCS]. Refined with iteration.
FCS_COP.1 /SHA /SIG_ECC /MAC_TDES /MAC_AES /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].

SFR	PP-eUICC	Security Target
FDP_ROL.1/FIREWALL		(A) Added from [PP-JCS].
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_ITC.2/Installer		(A) Added from [PP-JCS].
FMT_SMR.1/Installer		(A) Added from [PP-JCS].
FPT_FLS.1/Installer		(A) Added from [PP-JCS].
FPT_RCV.3/Installer		(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].

SFR	PP-eUICC	Security Target
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].
FCO_NRO.2/CM		(A) Added from [PP-JCS].
FDP_IFC.2/CM		(A) Added from [PP-JCS].
FDP_IFF.1/CM		(A) Added from [PP-JCS].
FDP_UIT.1/CM		(A) Added from [PP-JCS].
FIA_UID.1/CM		(A) Added from [PP-JCS].
FMT_MSA.1/CM		(A) Added from [PP-JCS].
FMT_MSA.3/CM		(A) Added from [PP-JCS].
FMT_SMF.1/CM		(A) Added from [PP-JCS].
FMT_SMR.1/CM		(A) Added from [PP-JCS].
FTP_ITC.1/CM		(A) Added from [PP-JCS].
FTP_ITC.1/CCM		(A) Added to cover secure card content management.
FAU_SAS.1		(A) Added to cover O.IC.PROOF_OF_IDEN-TITY.

SFR	PP-eUICC	Security Target
FPT_PHP.3		(A) Added to cover O.IC.SUPPORT.
FIA_UID.1/ITL		(A)
FIA_UAU.1/ITL		(A)
FIA_UAU.4/ITL		(A)
FDP_IFC.2/ITL		(A)
FDP_IFF.1/ITL		(A)
FDP_RIP.1/ITL		(A)
FMT_MSA.1/ITL		(A)
FMT_MSA.3/ITL		(A)
FMT_SMF.1/ITL		(A)
FMT_SMR.1/ITL		(A)
FPT_EMS.1/ITL		(A)
FPT_FLS.1/ITL		(A)
FTP_ITC.1/ITL		(A)

Table 10 Security Functional Requirement Consistency

2.4.3.9 SAR consistency

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

3. Security Problem Definition

This ST includes the SPD of [PP-eUICC] for the RSP part and the SPD of [PP-JCS] for the IC, OS and the Java Card System part.

3.1 Assets

All assets defined in [PP-eUICC], Section 3.1, are relevant for the TOE of this Security Target.

This ST includes the following additional assets:

All assets from [PP-JCS], Section 5.1.

D.UPDATE_IMAGE Encrypted and signed update image that contains the OS, personalised or not, with or without a profile.

D.TOE_IDENTIFIER Unique identifier of the composite TOE (currently installed TOE software + underlying chip hardware and firmware).

See section 2.4.3.1 for the complete list is assets.

3.2 Users and Subjects

All users and subjects defined in the [PP-eUICC], Section 3.2, are relevant for the TOE of this Security Target.

The following additional subjects are defined:

All subjects from [PP-JCS], Section 7.2.

S.SD A GlobalPlatform Security Domain representing on the card an off-card entity. This entity can be the Issuer, an Application Provider, the Controlling Authority or the Validation Authority.

S.ITL The Image Trusted Loader (ITL) provides secure functionality to update the TOE operating system with an image created by a trusted off-card entity.

See section 2.4.3.2 for the complete list of users and subjects.

3.3 Threats

All threats defined in the [PP-eUICC], Section 3.3, are relevant for the TOE of this Security Target. They have been refined by extending the list of directly threatened assets as shown in Table 11 (the additional assets are underlined).

Threat	**Directly threatened asset**
T.UNAUTHORIZED-PROFILE-MNG	D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYs, D.APP_CODE
T.UNAUTHORIZED-PLATFORM-MNG	D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYs, D.APP_CODE
T.PROFILE-MNG-INTERCEPTION	D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*., D.APP_C_DATA, D.APP_KEYs
T.PROFILE-MNG-ELIGIBILITY	D.TSF_CODE, D.DEVICE_INFO, D.EID, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYs, D.APP_CODE
T.UNAUTHORIZED-IDENTITY-MNG	D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, D.APP_CODE, D.APP_I_DATA, D.APP_C_DATA, D.APP_KEYs, D.SEC_DATA
T.IDENTITY-INTERCEPTION	D.SECRETS, D.EID, D.APP_C_DATA, , D.APP_KEYs

T.LOGICAL-ATTACK	D.TSF_CODE, D.PRO-FILE_NAA_PARAMS, D.PROFILE_POL-ICY_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, D.JCS_CODE, D.JCS_DATA, D.APP_CODE, D.API_DATA, D.SEC_DATA, D.CRYPTO, D.APP_I_DATA, D.APP_C_DATA, D.APP_KEYs

Table 11 Refined Threats

The following additional threats are defined:

T.ITL.UNAUTH *Load unauthorized version of Update Image*
The attacker tries to upload an unauthorized update image. Directly threatened asset(s): all assets.

T.ITL.CONFID *Confidentiality of Update Image during loading*
The attacker discloses (part of) the image used to update the TOE in the field while the image is transmitted to the card for installation. Directly threatened asset(s): D.UPDATE_IMAGE and the following assets defined in [PP-eUICC] that require protection from unauthorized disclosure: D.MNO_KEYS, D.PRO-FILE_NAA_PARAMS, D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS.

T.ITL.INTEG *Integrity of Update Image during loading*
The attacker modifies (part of) the image used to update the TOE in the field while the image is transmitted to the card for installation. Directly threatened asset(s): all assets.

T.ITL.INTERRUPT *ITL procedure interrupted*
The attacker tries to interrupt the ITL procedure leaving the TOE in a partially functional state. Directly threatened asset(s): all assets.

See section 2.4.3.3 for the complete list of threats.

3.4 Organisational Security Policies

The TOE complies with all Organisational Security Policies defined in the [PP-eUICC], Section 3.4.

This ST includes the following additional OSPs:

OSP.PROCESS-TOE *Identification of the TOE*

An identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

See section 2.4.3.4 for the complete list of OSPs.

3.5 Assumptions

All assumptions defined in the [PP-eUICC], Section 3.5, are included in this Security Target.

See section 2.4.3.5 for the complete list of Assumptions.

4. Security objectives

4.1 Security objectives for the TOE

The Security Objectives defined in the [PP-eUICC], Sections 4.1.1 – 4.1.5, are included in this Security Target.

This ST includes the following additional Security Objectives for the TOE:

O.ITL.SECURE_LOAD *Secure Loading of Update Image*
The TOE only installs update images that are encrypted, integrity-protected and signed by the authority in charge of delivering and installing updates. During the load phase of an update image, the TOE shall remain secure.

O.ITL.CONFID_KEYS *Confidentiality of the Update Keys*
The TOE keeps the cryptographic update keys secret, and is designed such that emissions from the TOE do not allow to read out or gain full or partial information about the keys.

O.TOE.IDENTIFICATION *Secure identification of the TOE*
The TOE provides means to store TOE identification data in its non-volatile memory and guarantees the integrity of these data.

See section 2.4.3.6 for the complete list of security objectives for the TOE.

4.2 Security objectives for the operational environment

The Security Objectives for the Operational Environment of this TOE are listed in section 2.4.3.7.

This ST includes the following additional Security Objectives for the Operational Environment:

OE.ITL.CONFID_IMAGE
The trusted off-card entity ensures that the update image is signed and transferred encrypted to the card and is not disclosed during the creation and

transfer. The keys used for signing and encrypting the image are kept confidential.

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

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

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

- PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.

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: o 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).

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-DPplus and OE.MNO

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-DPplus ensures that the credentials related to the secure channels will not be disclosed when used by off-card actors. O.DATA-INTEGRITY and O.RE.DATA-INTEGRITY ensure that the integrity of Device Info and eUICCInfo2 is protected at the eUICC level.

4.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

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

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

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

T.IDENTITY-INTERCEPTION

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

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

4.3.1.3 eUICC cloning

T.UNAUTHORIZED-eUICC

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

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

4.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

OE.TRUSTED-PATHS-LPAd ensures that the interfaces ES10a, ES10b and ES10c are trusted paths to the LPAd.

4.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS

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

4.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

- by the APIs provided by the Runtime Environment (O.RE.API);

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

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

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

The following objectives for the operational environment are also required:

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

T.PHYSICAL-ATTACK

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

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

In particular, the security objective O.IC.SUPPORT provides functionality to ensure atomicity of sensitive operations, secure low level access control and

protection against bypassing of the security features of the TOE. In particular, it explicitly ensures the independent protection in integrity of the Platform data.

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

4.3.2 Rationale Tables

4.3.2.1 Threats and Security Objectives

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

	CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD	
T.PROFILE-MNG-EL-IGIBILITY	OE.SM-DPplus, O.RE.SE-CURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 4.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, O.RE.DATA-CON-FIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 4.3.1.2
T.IDENTITY-INTER-CEPTION	OE.CI, O.INTERNAL-SE-CURE-CHANNELS, O.RE.SE-CURE-COMM	Section 4.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 4.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	Section 4.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 4.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.OP-ERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUP-	Section 4.3.1.6

	PORT, O.RE.DATA-CONFI-DENTIALITY, O.RE.DATA-IN-TEGRITY	
T.PHYSICAL-AT-TACK	O.IC.SUPPORT, O.IC.RE-COVERY, O.DATA-CONFI-DENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 4.3.1.6
T.ITL.CONFID	O.ITL.SECURE_LOAD, O.ITL.CONFID-KEYS, OE.ITL.CONFID_IMAGE	Counter the threat by ensuring that D.UP-DATE_IMAGE is not transferred in plain and that the keys are kept secret.
T.ITL.UNAUTH	O.ITL.SECURE_LOAD	Counter the threat by ensuring that only au-thorized updates can be loaded.
T.ITL.INTEG	O.ITL.SECURE_LOAD	Counters the threat by ensuring the authen-ticity and integrity of D.UPDATE_IMAGE during loading.
T.ITL.INTERRUPT	O.ITL.SECURE_LOAD, O.TOE.IDENTIFICATION	Counter the threat by ensuring that the TOE remains in a secure state after interruption of the ITL procedure, and that D.TOE_IDENTIFIER is only updated after

		successful completion of the ITL procedure.

Table 12 Threats and Security Objectives Coverage

Security Objectives	**Threats**
O.PPE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF-OF-IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION

OE.SM-DPplus	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.MNO	T.UNAUTHORIZED-PROFILE-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.PPE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UN-AUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK

OE.TRUSTED-PATHS-LPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
O.ITL.CONFID_KEYS	T.ITL.CONFID
O.ITL.SECURE_LOAD	T.ITL.UNAUTH, T.ITL.CONFID, T.ITL.INTEG, T.ITL.INTERRUPT
O.TOE.IDENTIFICATION	T.ITL.INTERRUPT
OE.ITL.CONFID_IMAGE	T.ITL.CONFID

Table 13 Security Objectives and Threats – Coverage

4.3.2.2 OSPs and Security Objectives

Organisational Security Policies	**Security Objective**	**Rationale**
OSP.LIFE-CYCLE	O.PPE-PPI, O.RE.PPE-PPI, O.OPERATE	[PP-eUICC], Section 4.3.2
OSP.PROCESS-TOE	O.TOE.IDENTIFICATION	The objective enforces this organisational security policy by ensuring that the TOE can be uniquely identified.

Table 14 OSPs and Security Objectives – Coverage

Security Objectives	Organisational Security Policies
O.PPE-PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF-OF-IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-DPplus	
OE.MNO	
O.IC.PROOF_OF_IDENTITY	
O.IC.SUPPORT	
O.IC.RECOVERY	
O.RE.PPE-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	
OE.APPLICATIONS	
OE.MNO-SD	
O.TOE.IDENTIFICATION	OSP.PROCESS-TOE
O.ITL.SECURE_LOAD	
O.ITL.CONFID_KEYS	
OE.ITL.CONFID_IMAGE	

Table 15 Security Objectives and OSPs – Coverage

4.3.2.3 Assumptions and Security Objectives for the Operational Environment

Assumptions	**Security Objectives for the Operational Environment**	**Rationale**
A.TRUSTED-PATHS-LPAd	OE.TRUSTED-PATHS-LPAd	[PP-eUICC], section 4.3.3
A.ACTORS	OE.CI, OE.SM-DPplus, OE.MNO	[PP-eUICC], section 4.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	[PP-eUICC], section 4.3.3

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

Security Objectives for the Operational Environment	**Assumptions**
OE.CI	A.ACTORS
OE.SM-DPplus	A.ACTORS

OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd
OE.MNO-SD	
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.ITL.CONFID_IMAGE	

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

5. Extended Requirements

The same extended component definition than [PP-eUICC] are defined in the current Security target:

- Extended Family FIA_API - Authentication Proof of Identity
- Extended Family FPT_EMS - TOE Emanation
- Extended Family FCS_RNG – Random number generation
- Extended Family FAU_SAS – Audit Data Storage

The extended components definition (FIA_API, FPT_EMS, FCS_RNG) from [PP-eUICC] is not repeated here. The same for FAU_SAS.1 which definition from [PP-0084] section 5.3 have been taken with no modification.

6. Security Requirements

The following SFRs are relevant for this TOE.

SFR	Included in this ST
[PP-eUICC] SFRs	All SFRs.
[PP-JCS] SFRs	All SFRs listed in section 2.4.3.8, added for secure RE support.
FPT_PHP.3	Added for secure IC support.
FTP_ITC.1/CCM	Added for secure RE support, in particular for providing secure means for card management activities.
FIA_UID.1/ITL FIA_UAU.1/ITL FIA_UAU.4/ITL FDP_IFC.2/ITL FDP_IFF.1/ITL FDP_RIP.1/ITL FMT_MSA.1/ITL FMT_MSA.3/ITL FMT_SMF.1/ITL FMT_SMR.1/ITL FPT_EMS.1/ITL FPT_FLS.1/ITL FTP_ITC.1/ITL	Added for secure post-issuance updates (ITL) support.

Table 18 SFRs of the TOE of this ST

6.1 eUICC Security Functional Requirements

6.1.1 Introduction

The TOE of this ST includes all SFRs contained in chapter 6.1.2-6.1.7 of [PP-eUICC] for the eUICC component in compliance with the Security Problem Definition stated in the [PP-eUICC].

The following assignments and selections are applicable. All other SFRs are included in the scope of the TOE of this ST without change (equivalent to the definition in [PP-eUICC]) and do not appear here.

6.1.2 Identification and authentication

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow

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

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

FIA_UAU.1/EXT Timing of authentication

FIA_UAU.1.1/EXT The TSF shall allow

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

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

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*]**[3] on behalf of the user to be performed before the user is identified.

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

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

FIA_USB.1/EXT User-subject binding

FIA_UAU.4/EXT Single-use authentication mechanisms

FIA_USB.1/MNO-SD User-subject binding

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

FIA_ATD.1/eUICC User attribute definition

FIA_API.1/eUICC Authentication Proof of Identity

6.1.3 Communication

FDP_IFF.1/SCP Simple security attributes

FDP_IFF.1.3/SCP The TSF shall enforce **[assignment: *no additional information flow control SFP rules*]**[4].

FDP_IFF.1.4/SCP The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[5].

FTP_ITC.1/SCP Inter-TSF 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)*****]**[6].

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

[4] [assignment: *additional information flow control SFP rules*]
[5] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[6] [assignment: *list of functions for which a trusted channel is required*]

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*]**[7].

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

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

- ***[SGP.22] §5.4.1 for commands and downloaded objects from U.MNO-OTA***
- ***[SGP.22] §5.5.1-5.5.5 for commands and downloaded objects from U.SM-DP+***
- ***[SGP.22] §5.7.3-5.7.22 for LPAd commands*]**[8]

when interpreting the TSF data from another trusted IT product.

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, LoadBoundProfilePackage*]**[9] that meets the following: **[assignment: *[GP] §11.8, [SGP.22] §5.7.6*]**[10].

FCS_CKM.4/SCP-SM Cryptographic key destruction

FCS_CKM.4.1/SCP-SM The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values*]**[11] that meets the following: **[assignment: *none*]**[12].

FCS_CKM.4/SCP-MNO Cryptographic key destruction

[7] [assignment: *additional importation control rules*]
[8] [assignment: *list of interpretation rules to be applied by the TSF*]
[9] [assignment: *key distribution method*]
[10] [assignment: *list of standards*]
[11] [assignment: *key distribution method*]
[12] [assignment: *list of standards*]

FCS_CKM.4.1/SCP-MNO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values*]**[13] that meets the following: **[assignment: *none*]**[14].

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

FDP_IFC.1/SCP Subset information flow control

FPT_TDC.1.1/SCP Inter-TSF basic TSF data consistency

FDP_UCT.1/SCP Basic data exchange confidentiality

FDP_UIT.1/SCP Data exchange integrity

FCS_CKM.1/SCP-SM Cryptographic key generation

Application Note 1: The TOEs underlying cryptography for the ElGamal elliptic curves key agreement (ECKA) is complaint with NIST P-256 (FIPS PUB 186-3 Digital Signature Standard) only.

6.1.4 Security Domains

FDP_ACF.1/ISDR Security attribute based access control

FDP_ACF.1.3/ISDR The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *ISDR shall perform the following operations:***

- ***ES8+.ConfigureISDP (Create and configure profile)***
- ***ES8+.StoreMetadata (Store profile metadata)***
- ***ES10c.EnableProfile (Enable profile)***
- ***ES10c.DisableProfile (Disable profile)***
- ***ES10c.DeleteProfile (Delete profile)***
- ***ES10c.eUICCMemoryReset (Perform a Memory reset)***

[13] [assignment: *key distribution method*]
[14] [assignment: *list of standards*]

***based on Profile "state" and profile policy rules "PPR"*]**[15].

FDP_ACF.1.4/ISDR The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: *when any of the defined rules by [SGP.22] related to Profile "state" hold and profile policy rules "PPR" do not hold*]**[16].

FDP_ACC.1/ECASD Subset access control

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

- **subjects: S.ISD-R,**
- **objects: S.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 (LPA – eUICC), creation of an eUICC signature on material provided by an ISD-R*]**[17]**.**

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"**
- **objects: 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 CI public key (PK.CI.ECDSA)**
  - **Creation of an eUICC signature on material provided by an ISD-R**

[15] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[16] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[17] [assignment: *additional list of subjects, objects, and operations between subjects and objects covered by the SFP*]

- **access to output data of these functions**
- **[assignment: *none*][18].**

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.22], Section 2.4*][19].**

FDP_ACF.1.3/ECASD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *none*]**[20].

FDP_ACF.1.4/ECASD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: *none*]**[21].

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

FDP_ACC.1/ISDR Subset access control

6.1.5 Platform Services

FDP_IFF.1/Platform_services Simple security attributes

[18] [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*]
[19] [assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[20] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[21] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_IFF.1.3/Platform_services The TSF shall enforce the **[assignment: *following additional information flow control SFP rules: none*]**[22].

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[23].

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*]**[24].

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.PPE, S.PPI or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **PPR and RAT enforcement**
  - **Network authentication**
- **[assignment: *none*]**[25]**.**

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

FDP_IFC.1/Platform_services Subset information flow control

6.1.6 Security management

FCS_RNG.1 Random number generation

[22] [assignment: *additional information flow control SFP rules*]
[23] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[24] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[25] [assignment: *other type of failure*]

FCS_RNG.1.1 The TSF shall provide a ***hybrid deterministic***[26] random number generator ***DRG.4***[27] 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*]**[28]

FCS_RNG.1.2 The TSF shall provide random numbers 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*]**[29].

FPT_EMS.1/eUICC TOE Emanation

FPT_EMS.1.1/eUICC The TOE shall not emit **[assignment: *information about IC power consumption, electromagnetic radiation, radio emission, internal state transition and timing during command execution]***[30] in excess of **[assignment: *non-useful information]***[31] enabling access to

- D.SECRETS;
- D.SK.EUICC.ECDSA

and the secret keys which are part of the following keysets:

- D.MNO_KEYS,

[26] [selection: *deterministic, hybrid deterministic, physical, hybrid physical*]
[27] [selection: *DRG.2, DRG.3, DRG.4, PTG.2, PTG.3*]
[28] [assignment: *list of security capabilities of the selected RNG class*]
[29] [assignment: *a defined quality metric of the selected RNG class*]
[30] [assignment: *types of emissions*]
[31] [assignment: *specified limits*]

- D.PROFILE_NAA_PARAMS.

FPT_EMS.1.2/eUICC The TSF shall ensure **[assignment: *unauthorised users]***[32] are unable to use the following interface **[assignment: *IC contact interface]***[33] to gain access to

- D.SECRETS;
- D.SK.EUICC.ECDSA

and the secret keys which are part of the following keysets:

- D.MNO_KEYS,
- D.PROFILE_NAA_PARAMS.

FMT_SMF.1/eUICC Specification of Management Functions

FMT_SMF.1.1/eUICC The TSF shall be capable of performing the following management functions: **[assignment: *Profile Management functions specified in [SGP.22]]*** [34].

FDP_SDI.1/eUICC Stored data integrity monitoring

FDP_SDI.1.1/eUICC 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 assets of the Security Target TOE that require to be protected against unauthorized modification, including but not limited to the assets of the [PP-eUICC] that require to be protected against unauthorized modification:

- D.MNO_KEYS
- Profile data
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE_POLICY_RULES
  - D.PROFILE_USER_CODES

[32] [assignment: *types of emissions*]
[33] [assignment: *specified limits*]
[34] [assignment: *list of management functions to be provided by the TSF*]

- Management data
  - D.PLATFORM_DATA
  - D.DEVICE_INFO
  - D.PLATFORM_RAT
- Identity management data
  - D.SK.EUICC.ECDSA
  - D.CERT.EUICC.ECDSA
  - D.PK.CI.ECDSA
  - D.EID
  - D.SECRETS
  - D.CERT.EUM.ECDSA
  - D.CRLs if existing
- D.TOE_IDENTIFIER

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

FDP_RIP.1/eUICC Subset residual information protection

FPT_FLS.1/eUICC Failure with preservation of secure state

FMT_MSA.1/PLATFORM_DATA Management of security attributes

FMT_MSA.1/PPR Management of security attributes

FMT_MSA.1/CERT_KEYS Management of security attributes

FMT_SMR.1/eUICC Security roles

FMT_MSA.1/RAT Management of security attributes

FMT_MSA.3/eUICC Static attribute initialisation

6.1.7 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, Tuak, *Cave***[35] 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.**
- ***Cave according to standard [CAVE] with the following restrictions:***
  - ***Supports 0~16 rounds of SSD Generation***[36]**.**

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]***[37] that meets the following: **[assignment: *[SGP.22] §3.1.3, §5.7.6, [SIMalliance], §8.6.3]***[38].

FCS_CKM.4/Mobile_network Cryptographic key destruction

[35] [selection: *other algorithm, no other algorithm*]
[36] [selection: *other algorithm, no other algorithm*]
[37] [assignment: *cryptographic key distribution method*]
[38] [assignment: *list of standards*]

FCS_CKM.4.1/Mobile_network The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting keys with zero values]***[39] that meets the following: **[assignment: *none]***[40].

[39] [assignment: *cryptographic key destruction method*]
[40] [assignment: *list of standards*]

6.2 Java Card System SFRs

In the Protection Profile [PP-eUICC] the objectives for the Runtime Environment are defined as objectives for the environment (OE.RE.*). Since the IC and the RE is part of the TOE of this ST, the objectives for the environment were translated into objectives for the TOE (as shown in section 4.1). They subsequently have to be covered by SFRs that have been imported here from the Java Card PP [PP-JCS] (as shown in section 2.4.3.8). The following subsections address only those SFRs where assignments and selections were made by the ST author.

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

6.2.1 CoreG_LC Security Functional Requirements

6.2.1.1 Firewall Policy

FDP_IFF.1/JCVM Simple security attributes

FDP_IFF.1.3/JCVM The TSF shall enforce the **[assignment: *following additional information flow control SFP rules: none*]**[41].

FDP_IFF.1.4/JCVM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none*]**[42].

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **[assignment: *none*]**[43].

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

FDP_ACC.2/FIREWALL Complete access control

FDP_ACF.1/FIREWALL Security attribute based access control

[41] [assignment: *additional information flow control SFP rules*]
[42] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[43] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

FDP_IFC.1/JCVM Subset information flow control

FDP_RIP.1/OBJECTS Subset residual information protection

FMT_MSA.1/JCRE Management of security attributes

FMT_MSA.1/JCVM Management of security attributes

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

FMT_MSA.3/FIREWALL Static attribute initialisation

FMT_MSA.3/JCVM Static attribute initialisation

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

FMT_SMF.1/RE Specification of Management Functions

FMT_SMR.1/RE Security roles

6.2.1.2 Application Programming Interface

FCS_CKM.1 Cryptographic key generation

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

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

FCS_CKM.4/RE Cryptographic key destruction

FCS_CKM.4.1/RE The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: *physically overwriting the keys with zero values]***[44] that meets the following: **[assignment: *none]***[45].

FCS_COP.1 Cryptographic operation

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

[44] [assignment: *cryptographic key destruction method*]
[45] [assignment: *list of standards*]

Iteration	Operation	Algo-rithm	Key sizes	List of standards
/SHA	hashing	SHA-256, 384, 512	n.a.	[FIPS180-4]
/SIG_ECC	digital sig-nature generation and verifi-cation	ECDSA	256 bits	[FIPS186-4] [BSI TR 03111] [RFC5639]
/MAC_TDES	MAC gen-eration and verification	Triple-DES CBC MAC	112, 168 bits	[FIPS46-3], Chapter 'TRI-PLE 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
/CIPH_TDES	encryption and de-cryption	Triple-DES in CBC	112, 168 bits	[SP800-67] [SP800-38a]
/CIPH_AES		AES in CBC and ECB modes	128, 192, 256 bits	[FIPS197] [SP800-38a]
/CIPH_AES_GCM		AES in GCM mode	128 bits	[FIPS197] [SP800-38d]

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

Application Note 2: The cryptographic algorithms stated below of FCS_COP.1 are not provided as a service via JavaCard API.
FCS_COP.1 supports the requirements of [SGP.22] related to cryptographic mechanisms used for:

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

- *A U.SM-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 defined in [RFC3447] §2.4.3, or optionally SCP81 according to [GP AM B] using the parameters defined in [RFC3447] §2.4.4 (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO).*

(2) Establishment of and secure communication over trusted channels (FTP_ITC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP) by providing the required cryptographic algorithms for the SCP-SGP22, SCP80 and SCP81.

FCS_COP.1 further covers the requirements related to cryptographic mechanisms used for post-delivery code loading:

- *decryption and MAC verification during the loading (/CIPH_AES_GCM),*
- *verification of signature over the update image after loading (/MAC_AES for CMAC),*
- *verification of the hash over the update image after loading (/SHA for SHA-256).*

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

FDP_RIP.1/ABORT Subset residual information protection

FDP_RIP.1/APDU Subset residual information protection

FDP_RIP.1/bArray Subset residual information protection

FDP_RIP.1/GlobalArray Subset residual information protection

FDP_RIP.1/KEYS Subset residual information protection

FDP_RIP.1/TRANSIENT Subset residual information protection

FDP_ROL.1/FIREWALL Basic rollback

6.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

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

- **throw an exception,**
- **lock the card session,**
- **reinitialize the Java Card System and its data**
- **[assignment: *other actions: Card Lock / Application Lock]***[46]

upon detection of a potential security violation.

Refinement:

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

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)]***[47].

Application Note 3: Bytecode verification is performed off-card.

FDP_SDI.2/DATA Stored data integrity monitoring and action

FDP_SDI.2.1/DATA The TSF shall monitor user data stored in containers controlled by the TSF for **[assignment: integrity errors]**[48] on all objects, based on the following attributes: **[assignment: *checksum integrity (complementary value, Error Detection Code) of cryptographic keys, PIN values and their associated attributes]***[49].

FDP_SDI.2.2/DATA Upon detection of a data integrity error, the TSF shall **[assignment: *bring the card into a secure state]***[50].

FPR_UNO.1 Unobservability

[47] [assignment: *list of other runtime errors*]
[48] [assignment: integrity errors]
[49] [assignment: *user data attributes*]
[50] [assignment: *actions to be taken*]

FPR_UNO.1.1 The TSF shall ensure that **[assignment: *unauthorized users or subjects]***[51] are unable to observe the operation **[assignment: *cryptographic operations, comparison operations]***[52] on **[assignment: *key values, PIN values]***[53] by **[assignment: *S.JCRE, S.Applet, S.SD, S.ITL]***[54].

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

FPT_TDC.1.2/RE The TSF shall use

- **the rules defined in [JCVM] specification,**
- **the API tokens defined in the export files of reference implementation**,
- **[assignment: *no other rules]***[55]

when interpreting the TSF data from another trusted IT product.

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

FPT_FLS.1/RE Failure with preservation of secure state

6.2.1.4 AID Management

FIA_USB.1/AID User-subject binding

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: *rules defined in FMT_MSA.2/FIREWALL_JCVM and FMT_MSA.3.1/FIREWALL]***[56].

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

[51] [assignment: *list of users and/or subjects*]
[52] [assignment: *list of operations*]
[53] [assignment: *list of objects*]
[54] [assignment: *list of protected users and/or subjects*]
[55] [assignment: *list of interpretation rules to be applied by the TSF*]
[56] [assignment: *list of rules for the initial association of attributes*]

behalf of users: **[assignment: *rules defined in FMT_MSA.3.1/FIREWALL*]**[57].

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

FIA_ATD.1/AID User attribute definition

FIA_UID.2/AID User identification before any action

FMT_MTD.1/JCRE Management of TSF data

FMT_MTD.3/JCRE Secure TSF data

6.2.2 InstG Security Functional Requirements

FPT_RCV.3/Installer Automated recovery without undue loss

FPT_RCV.3.1/Installer When automated recovery from **[assignment: *power loss*]**[58] 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/Installer For **[assignment: *a failure during load/installation of a package/applet and deletion of a package/applet/object*]**[59], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/Installer 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%]**[60] for loss of TSF data or objects under the control of the TSF.

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

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

[57] [assignment: *list of rules for the changing of attributes*]
[58] [assignment: *list of failures/service discontinuities*]
[59] [assignment: *list of failures/service discontinuities*]
[60] [assignment: *quantification*]

FMT_SMR.1/Installer Security roles

FPT_FLS.1/Installer Failure with preservation of secure state

6.2.3 ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

FDP_ACF.1/ADEL Security attribute based access control

FDP_RIP.1/ADEL Subset residual information protection

FMT_MSA.1/ADEL Management of security attributes

FMT_MSA.3/ADEL Static attribute initialisation

FMT_SMF.1/ADEL Specification of Management Functions

FMT_SMR.1/ADEL Security roles

FPT_FLS.1/ADEL Failure with preservation of secure state

6.2.4 ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

FPT_FLS.1/ODEL Failure with preservation of secure state

6.2.5 CarG Security Functional Requirements

FCO_NRO.2/CM Enforced proof of origin

FCO_NRO.2.3/CM The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given **[assignment: *that the data origin authentication provided within the context of secure messaging was successful]***[61].

Application Note 4: FCO_NRO.2/CM is related to secure messaging by means of GlobalPlatform Secure Channel Protocol. In the context of secure messaging, message integrity also provides data origin authentication ([GP],

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

Section 10.5). The TOE performs verification of the origin of the package by applying command MAC verification. No evidence is kept on the card for future verifications.

FDP_IFF.1/CM Simple security attributes

FDP_IFF.1.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** based on the following types of subject and information security attributes **[assignment:**

(1) The keys used by the subject S.SD acting on behalf of the off-card entity to decrypt and verify received messages;

(2) *Authentication retry counter]*[62]**.**

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

1. ***The subject S.SD shall accept a message only if it comes from the subject S.CAD;***
2. ***The subject S.SD shall accept an application CAP file only if it has received all the APDUs sent by the subject S.CAD without modification and in the right order;***
3. ***Secure Channel initiation is only possible if the authentication retry counter limit is not exceeded]***[63].

FDP_IFF.1.3/CM The TSF shall enforce the **[assignment: *following additional information flow control SFP rules: Runtime behaviour rules defined by GlobalPlatform for the following card management functions:***

- ***loading (Section 9.3.5 of [GP]);***
- ***installation (Section 9.3.6 of [GP]);***
- ***extradition (Section 9.4.1 of [GP]);***
- ***personalization of an application or a Security Domain (Section 3.3.2 of [GP UICC]);***
- ***deletion (Section 9.5 of [GP]);***

[62] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[63] [assignment: *the rules describing the communication protocol used by the CAD and the card for transmitting a new CAP file*]

- ***privileges update of an application or a Security Domain ([GP UICC])]***[64].

FDP_IFF.1.4/CM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none]***[65].

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

- **The TOE fails to verify the integrity and authenticity evidences of the application CAP file.**
- **[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]***[66]**.**

FDP_UIT.1/CM Data exchange integrity

FDP_UIT.1.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** to ***receive***[67] user data in a manner protected from ***modification, replay, insertion and deletion***[68] errors.

FIA_UID.1/CM Timing of identification

FIA_UID.1.1/CM The TSF shall allow **[assignment:**

- ***application selection;***
- ***initiating communication a trusted channel]***[69]

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

[64] [assignment: *additional information flow control SFP rules*]
[65] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[66] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[67] [selection: *transmit, receive*]
[68] [selection: *modification, deletion, insertion, replay*]
[69] [assignment: *list of TSF-mediated actions*]

FMT_MSA.1/CM Management of security attributes

FMT_MSA.1.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** to restrict the ability to ***modify, delete, reset***[70] the security attributes **[assignment: *Secure Channel static keys, the Secure Channel security level and the Secure Channel protocol of a Security Domain, Secure Channel session keys, Sequence Counter, ICV, authentication retry counter]***[71] to **[assignment: *an authenticated off-card entity associated with the S.SD]***[72].

FMT_MSA.3/CM Static attribute initialisation

FMT_MSA.3.2/CM The TSF shall allow the **[assignment: *following authorised identified roles: S.SD]***[73] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/CM Specification of Management Functions

FMT_SMF.1.1/CM The TSF shall be capable of performing the following management functions: **[assignment: *card management functions listed in FDP_IFF.1.3/CM]***[74].

FMT_SMR.1/CM Security roles

FMT_SMR.1.1/CM The TSF shall maintain the roles: **[assignment: *S.SD, S.CAD]***[75].

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

FDP_IFC.2/CM Complete information flow control

[70] [selection: *change_default, query, modify, delete, [assignment: other operations]*]
[71] [assignment: *list of security attributes*]
[72] [assignment: *the authorised identified roles*]
[73] [assignment: *the authorised identified roles*]
[74] [assignment: *list of management functions to be provided by the TSF*]
[75] [assignment: *the authorised identified roles*]

FTP_ITC.1/CM Inter-TSF trusted channel

6.3 Card Content Management SFRs

The Runtime Environment shall provide secure means for card management activities ([PP-eUICC], section 4.2.2, OE.RE.PPE-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.PPE-PPI) and subsequently have to be covered by SFRs. Therefore the following SFRs are introduced.

FTP_ITC.1/CCM Inter-TSF trusted channel

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

FTP_ITC.1.3/CCM The TSF shall initiate communication via the trusted channel for **[assignment: *all card management functions listed in FDP_IFF.1.3/CM]***[76].

6.4 Secure IC Platform SFRs

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

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

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist ***physical manipulation and physical probing*** to the ***TSF*** by responding automatically such that the SFRs are always enforced.

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide ***the process before TOE Delivery***[77] with the capability to store ***Initialisation Data***[78] in the ***NVM***[79].

Application note 5: Initialisation Data is data that is loaded by the Initialiser during eUICC lifecycle phase b.

6.5 ITL SFRs

The following SFR provide secure OS update proprietary features related SFRs.

6.5.1 Class FIA: Identification and Authentication

FIA_UID.1/ITL Timing of Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/ITL The TSF shall allow **[assignment:**

1) ***to establish a communication channel*****,**
2) ***query the TOE version (D.TOE_IDENTIFIER)]***[80]

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

FIA_UID.1.2/ITL 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/ITL Timing of Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of Identification **fulfilled** by FIA_UID.1/ITL

[77] [assignment: *list of subjects*]
[78] [selection: *the Initialisation Data, Pre-personalisation Data, [assignment: other data]*]
[79] [assignment: *type of persistent memory*]
[80] [assignment: *list of TSF-mediated actions]*

FIA_UAU.1.1/ITL The TSF shall allow **[assignment:**

1) ***to establish a communication channel*****,**
2) ***query the TOE version (D.TOE_IDENTIFIER)]***[81]

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

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

FIA_UAU.4/ITL Single-use authentication mechanisms (ITL)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1/ITL The TSF shall prevent reuse of authentication data related to **[assignment: *the authentication mechanism used to load D.UPDATE_IMAGE]***[82].

Application note 6: Authentication is implicit through the secure channel establishment for SCP03t or AES GCM.

6.5.2 Class FDP: User Data Protection

FDP_IFC.2/ITL Complete information flow control (ITL)

Hierarchical to: FDP_IFC.1 Subset information flow control.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/ITL The TSF shall enforce the **[assignment: *ITL information flow control SFP]***[83] on **[assignment: *S.ITL, D.UPDATE_IMAGE]***[84] **and all** operations **that** cause that information to flow to and from subjects covered by the **SFP**.

FDP_IFC.2.2/ITL 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.

[81] [assignment: *list of TSF-mediated actions*]
[82] [assignment: *identified authentication mechanism(s)*]
[83] [assignment: *information flow control SFP*]
[84] [assignment: *list of subjects and information*]

FDP_IFF.1/ITL Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1/ITL The TSF shall enforce the **[assignment: *ITL information flow control SFP]***[85] based on the following types of subject and information security attributes **[assignment:**

- ***S.ITL with security attributes:***
  - ***Current Transaction ID, ongoing Transaction ID,***
  - ***ITL encryption key and ITL MAC key (AES-ENC.EUICC.AUTH / AES-MAC.EUICC.AUTH),***
  - ***ITL signature key (AES-MAC.OWN.SIGN).***
- ***D.UPDATE_IMAGE with security attributes:***
  - ***Update image version number,***
  - ***Update image checksum*.]**[86]

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

1. ***The off-card entity has established a secure channel with the S.ITL*.**
2. ***The TOE shall only accept update images sent via a secure channel.***
3. ***The TOE shall only accept update images which signature can be verified with the ITL signature key]***[87].

Application Note 7: SCP03t or AES GCM variants are used as secure channel protocol.

[85] [assignment: *information flow control SFP*]
[86] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[87] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

FDP_IFF.1.3/ITL The TSF shall enforce the ***following additional information flow control SFP rules*: *S.ITL shall only authorize D.UPDATE_IMAGE for the update process if the following rules apply:***

1. ***The version number of the update image shall be greater than the version of the installed corresponding software image. If the condition is verified, proceed with opening of the secure channel and establishment of secure channel keys (loading phase), otherwise abort.***
2. ***The ongoing Transaction ID shall be greater than the current Transaction ID. If the condition is verified, the current Transaction ID is set to invalid (00…00) and proceed with 3, otherwise abort.***
3. ***The TSF shall be able to load the image, decrypt the image data package and check the integrity and authenticity of the update image (FCS_COP.1/CIPH_AES_GCM). If the integrity and authenticity are not both validated, abort and erase all session data transferred so far (FDP_RIP.1/ITL). Step 3 is performed in loop until the entire update image is loaded.***
4. ***After loading of the image is finished, the TSF shall verify the checksum (SHA-256 hash, FCS_COP.1/SHA) over the loaded image. If successful proceed with 5, otherwise abort and erase all session data that was transferred so far (FDP_RIP.1/ITL).***
5. ***The TSF shall verify the authenticity of the loaded image (CMAC verification, FCS_COP.1/MAC_AES). If successful a valid current Transaction ID is stored and a reset is performed. After reset the OS takes over the operation***[88]*.*

FDP_IFF.1.4 /ITL The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: *none]***[89].

FDP_IFF.1.5/ITL The TSF shall explicitly deny an information flow based on the following rules: **[assignment:**

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

- ***The TOE shall reject communication between off-card entity and S.ITL if it is not performed in a secure channel]***[90].

FDP_RIP.1/ITL Subset Residual Information Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1/ITL The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***deallocation of the resource from***[91] the following objects: **[assignment: *ITL secure channel keys (immediately after closing related communication session)]***[92]***.***

6.5.3 Class FMT: Security Management

FMT_MSA.1/ITL Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/ITL The TSF shall enforce the **[assignment: *ITL information flow control SFP]***[93] to restrict the ability to ***modify***[94] the security attributes **[assignment: *current Transaction ID]***[95] to **[assignment: *S.ITL]***[96].

FMT_MSA.3/ITL Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

---

[90] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[91] [selection: *allocation of the resource to, deallocation of the resource from*]
[92] [assignment: *list of objects*]
[93] [assignment: *access control SFP(s), information flow control SFP(s)*]
[94] [assignment: *selection: change_default, query, modify, delete, [assignment: other operations]*]
[95] [assignment: *list of security attributes*]
[96] [assignment: *authorised identified roles*]

FMT_MSA.3.1/ITL The TSF shall enforce the **[assignment: *ITL information flow control SFP*]**[97] to provide ***restrictive***[98] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ITL The TSF shall allow the **[assignment: *S.ITL*]**[99] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/ITL Specification of Management Functions including Updates

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/ITL The TSF shall be capable of performing the following management functions: **[assignment: *query the update image version number, query the current Transaction ID*]**[100].

FMT_SMR.1/ITL Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification: fulfilled by FIA_UID.1/ITL

FMT_SMR.1.1/ITL The TSF shall maintain the roles **[assignment: *S.ITL*]**[101].

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

6.5.4 Class FPT: Protection of the TSF

FPT_EMS.1/ITL TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

[97] [assignment: *access control SFP, information flow control SFP*]
[98] [assignment: *selection, choose one of: restrictive, permissive, [assignment: other property]*]
[99] [assignment: *authorized identified roles*]
[100] [assignment: *list of management functions to be provided by the TSF*]
[101] [assignment: *the authorized identified roles*]

FPT_EMS.1.1/ITL The TOE shall not emit **[assignment: *information about IC power consumption, electromagnetic radiation and command execution time]***[102] in excess of **[assignment: *non-useful information]***[103] enabling access to **[assignment: *ITL encryption key and MAC key, ITL signature key used for the update mechanism]***[104] and **[assignment: *none]***[105].

FPT_EMS.1.2/ITL The TSF shall ensure **[assignment: *any users]***[106] are unable to use the following interface **[assignment: *contact-based interface and circuit contacts]***[107] to gain access to **[assignment: *ITL encryption and ITL MAC key, ITL signature key, current Transaction ID used for the update mechanism]***[108] and **[assignment: *none]***[109].

FPT_FLS.1/ITL Failure with Preservation of Secure State (Failed Update)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1/ITL The TSF shall preserve a secure state when the following types of failures occur **[assignment:**

1) ***Failure during a transmission of the update image.***
2) ***Interruption of the ITL process.***
3) ***Failure detected after loading the update image]***[110]***.***

6.5.5 Class FTP: Trusted Path/Channels

FTP_ITC.1/ITL Inter-TSF trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

[102] [assignment: *types of emissions*]
[103] [assignment: *specified limits*]
[104] [assignment: *list of types of TSF data*]
[105] [assignment: *list of types of user data*]
[106] [assignment: *type of users*]
[107] [assignment: *types of connections*]
[108] [assignment: *list of types of TSF data*]
[109] [assignment*: list of types of user data*]
[110] [assignment: *list of types of failures in the TSF*]

FTP_ITC.1.1/ITL 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/ITL The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.
FTP_ITC.1.3/ITL The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for **[assignment: *any data exchange between the TOE and the authenticated off-card entity initiating the ITL procedure]***[111].

6.6 Security Requirements Dependencies

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

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

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

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

Security Functional Requirement	**Dependencies**	**Satisfied Dependencies**
FCS_COP.1/SIG_ECC In case the public key included in its certificates CERT.DPauth.ECDSA and CERT.DPpb.ECDSA is based on brainpoolP256r1.	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4

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

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) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_PHP.3	No Dependencies	-
FTP_ITC.1/CCM	No Dependencies	-
FIA_UID.1/ITL	No Dependencies	-
FIA_UAU.1/ITL	FIA_UID.1 Timing of Identification	FIA_UID.1/ITL
FIA_UAU.4/ITL	No Dependencies	-
FDP_IFC.2/ITL	FDP_IFF.1 Simple security attributes	FDP_IFF.1/ITL
FDP_IFF.1/ITL	FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/ITL, FMT_MSA.3/ITL
FDP_RIP.1/ITL	No Dependencies	-
FMT_MSA.1/ITL	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/ITL, FMT_SMR.1/ITL, FMT_SMF.1/ITL

FMT_MSA.3/ITL	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_MSA.1/ITL, FMT_SMR.1/ITL
FMT_SMF.1/ITL	No Dependencies	-
FMT_SMR.1/ITL	FIA_UID.1 Timing of identification	FIA_UID.1/ITL
FPT_EMS.1/ITL	No Dependencies	-
FPT_FLS.1/ITL	No Dependencies	-
FTP_ITC.1/ITL	No Dependencies	-

Table 19 Extension of SFR Dependencies

6.7 Security Funcitonal Requirements Rationale

6.7.1 SFRs for eUICC rationale

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

6.7.2 SFRs for Runtime Environment rationale

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

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

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

RE objectives	Translation from Java Card PP
O.RE.PPE-PPI	O.INSTALL, O.DELETION, O.LOAD
O.RE.SECURE-COMM	O.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION
O.RE.API	O.CARD-MANAGEMENT, O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM
O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.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.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE

OE.SCP.RECOVERY and OE.SCP.SUPPORT from [PP-JCS] are equivalent to OE.IC.RECOVERY and OE.IC.SUPPORT from [PP-eUICC] converted to

O.IC.RECOVERY and O.IC.SUPPORT in current Security Target. See next section for the rationale.

6.7.3 SFRs for Underlying platform IC rationale

Objective	**SFRs**	**Rationale / statement on contribution to the objective coverage**
O.IC.SUPPORT	FCS_CKM.1/*, FCS_CKM.4/RE, FAU_ARP.1, FPR_UNO.1, FPT_EMS.1/*, FPT_PHP.3, FDP_SDI.2/DATA, FDP_ROL.1/FIREWALL	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	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 20 IC Security Objectives and SFRs – Coverage

6.7.4 SFRs for ITL rationale

Objective	**SFRs**	**Rationale / statement on contribution to the objective coverage**
O.ITL.SECURE_LOAD	FCS_COP.1/SHA, FCS_COP.1/MAC_AES, FCS_COP.1/ CIPH_AES_GCM, FCS_CKM.1/AES, FIA_UID.1/ITL, FIA_UAU.1/ITL, FIA_UAU.4/ITL, FDP_IFF.1/ITL, FDP_IFC.2/ITL, FPT_FLS.1/ITL, FPT_ITC.1/ITL, FMT_MSA.1/ITL, FMT_MSA.3/ITL, FMT_SMR.1/ITL	Contribute to the coverage of the objective: by providing secure cryptographic mechanisms for the ITL procedure (FCS_COP.1/SHA, /MCA_AES, /CIPH_AES_GCM and FCS_CKM.1/AES); by requiring identification (FIA_UID.1/ITL) and authentication (FIA_UAU.1/ITL) prior to post-issuance updates; by enforcing a trusted channel for data exchange between the TOE and the authenticated off-card entity initiating the ITL procedure (FPT_ITC.1/ITL) by letting S.ITL handle the ITL procedure (FMT_SMR.1/ITL) and applying the rules of the Information Flow Control policy (FDP_IFF.1/ITL) and enforcing restrictive default values for the attributes of the ITL information flow control SFP (FMT_MSA.3/ITL); by ensuring that only allowed versions of the D.UPDATE_IMAGE are accepted and by checking the evidence data of authenticity and integrity (FDP_IFC.2/ITL);

		by ensuring a secure state after interruption (FPT_FLS.1/ITL); by enforcing authenticity and integrity of update image (FIA_UAU.4/ITL); by allowing to modify the current Transaction ID only after successful update procedure and only by S.ITL (FMT_MSA.1/ITL);
O.ITL.CONFID_KEYS	FPT_EMS.1/ITL, FDP_RIP.1/ITL, FPR_UNO.1	Contribute to the coverage of the objective by ensuring the unobservability and confidentiality of the keys used for post-issuance updates.
O.TOE.IDENTIFICATION	FDP_SDI.1/eUICC, FMT_SMF.1/ITL	Contribute to cover the objective by storing the identification data (D.TOE_IDENTIFIER) in an integrity protected manner, and by providing the ability to query the identification data of the TOE.

Table 21 ITL Security Objectives and SFRs – Coverage

7. TOE Summary Specification (ASE_TSS)

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

7.1 SF.TRANSACTION

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

7.2 SF.ACCESS_CONTROL

This TSF is responsible for enforcing the following security policies:

- ISD-R access control SFP
- ISD-P content access control SFP
- ECASD access control SFP
- FIREWALL access control SFP
- ADEL access control SFP
- JCVM information flow policy
- CAP FILE LOADING information flow control SFP
- ITL 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 restrictive default values (FMT_MSA.3);
- Management of roles and security functions (FMT_SMR.1 and FMT_SMF.1).

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

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

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

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

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

The TSF enforces the rules under which
- the S.ISD-R can perform its functions (ISD-R access control SFP in FDP_ACC.1/ISDR and FDP_ACF.1/ISDR),
- the S.ISD-R can perform ECASD functions and obtain output data from these functions (ECASD access control SFP in FDP_ACC.1/ECASD and FDP_ACF.1/ECASD).

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

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

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

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

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

7.3 SF.INTEGRITY

This TSF provides protection from integrity errors.

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

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

7.4 SF.SECURITY

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

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

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

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

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

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

The TOE preserves a secure state

- when platform or content management operations fail, e.g.
    - failure of creation of a new ISD-P by ISD-R,
    - failure of installation of a profile by ISD-R,
    - the installer fails to load/install a CAP file/applet,
    - the applet deletion manager fails to delete a CAP file/applet,
    - the object deletion functions fail to delete all the unreferenced objects owned by the applet that requested the execution of the method.
- upon failures that lead to a potential security violation during the processing of a S.PPE, S.PPI or S.TELECOM API specific functions,

- upon failures detected during post-issuance update process (ITL),
- upon detection of a potential security violation described in FAU_ARP.1.

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

7.5 SF.PLATFORM_MANAGEMENT

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

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

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

Content changes are permitted according to the privileges that have been assigned to the acting Security Domain that holds cryptographic keys used to

support the Secure Channel Protocol operations and/or to authorize platform management functions. Before performing platform or content management operations, the TOE checks if the off-card entity has been successfully authenticated and a Secure Channel Session has been successfully initiated. Secure communication is provided by SF.SECURE_CHANNEL.

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

7.6 SF.SECURE_CHANNEL

This TSF is related to the protection of:

- Profiles downloaded from SM-DP+,
- Commands received from SM-DP+ and MNO OTA Platform,
- PPR received from the MNO OTA Platform,
- CAP file loading,
- Post-issuance Update image loading

by enforcing the following security policies:

- Secure Channel Protocol information flow control SFP,
- CAP FILE LOADING information flow control SFP
- ITL 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, SCP03(t), 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]
SCP03(t)	AES in CBC, AES CMAC, AES in GCM mode used by ITL procedure
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

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

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

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

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

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

The ITL component uses the AES GCM or SCP03t encryption scheme.

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

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

7.7 SF.CRYPTO

This TSF controls all the operations related to the cryptographic key management (generation, distribution, destruction) and cryptographic operations (FCS_CKM.1/*, FCS_CKM.2/*, FCS_CKM.4/*, FCS_COP.1/*).

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

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

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

Key distribution is provided by the following means:

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

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

The TOE provides the following algorithms for hashing:

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

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

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

The TOE provides key agreement:

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

The TOE provides MAC generation and verification:

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

The TOE provides encryption and decryption:

- Triple-DES in CBC mode as required by SCP02,
- AES in CBC mode as required by FDP_IFF.1/SCP (SCP80/81, SCP-SGP.22), FDP_UCT.1/SCP, SCP03, SCP03(t).
- AES in GCM mode used by ITL procedure for SCP03(t).

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

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

7.8 SF.RNG

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

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

7.9 SF.IDENTITY

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

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

7.10 TSS Rationale

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

7.10.1 eUICC SFRs coverage

Security Functional Requirement	**Coverage by TSS Security Function(s)**
FIA_UID.1/EXT	SF.ACCESS_CONTROL
FIA_UAU.1/EXT	SF.ACCESS_CONTROL
FIA_USB.1/EXT	SF.ACCESS_CONTROL
FIA_UAU.4/EXT	SF.ACCESS_CONTROL
FIA_UID.1/MNO-SD	SF.ACCESS_CONTROL
FIA_USB.1/MNO-SD	SF.ACCESS_CONTROL
FIA_ATD.1/eUICC	SF.ACCESS_CONTROL
FIA_API.1.1/eUICC	SF.CRYPTO 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.4/SCP-SM	SF.CRYPTO

Security Functional Requirement	Coverage by TSS Security Function(s)
FCS_CKM.4/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/eUICC	SF.SECURITY
FDP_SDI.1/eUICC	SF.INTEGRITY
FDP_RIP.1/eUICC	SF.SECURITY
FPT_FLS.1/eUICC	SF.SECURITY
FMT_MSA.1/PLATFORM_DATA	SF.ACCESS_CONTROL
FMT_MSA.1/PPR	SF.ACCESS_CONTROL
FMT_MSA.1/CERT_KEYS	SF.ACCESS_CONTROL
FMT_SMF.1/eUICC	SF.ACCESS_CONTROL
FMT_SMR.1/eUICC	SF.ACCESS_CONTROL
FMT_MSA.1/RAT	SF.ACCESS_CONTROL

Security Functional Requirement	Coverage by TSS Security Function(s)
FMT_MSA.3/eUICC	SF.ACCESS_CONTROL
FCS_COP.1/Mobile_network	SF.CRYPTO
FCS_CKM.2/Mobile_network	SF.CRYPTO
FCS_CKM.4/Mobile_network	SF.CRYPTO

7.10.2 Runtime Environment SFRs coverage

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

/ECC /Triple DES /AES	
FCS_CKM.4/RE	SF.CRYPTO
FCS_COP.1 /SHA /SIG_ECC /MAC_TDES /MAC_AES /CIPH_TDES /CIPH_AES /CIPH_AES_GCM /ECKA-EG	SF.CRYPTO
FDP_RIP.1/ABORT	SF.TRANSACTION
FDP_RIP.1/APDU	SF.SECURITY
FDP_RIP.1/bArray	SF.SECURITY
FDP_RIP.1/GlobalArray	SF.SECURITY
FDP_RIP.1/KEYS	SF.SECURITY
FDP_RIP.1/TRANSIENT	SF.SECURITY
FDP_ROL.1/FIREWALL	SF.TRANSACTION
FAU_ARP.1	SF.SECURITY
FDP_SDI.2/DATA	SF.INTEGRITY

FPR_UNO.1	SF.SECURITY
FPT_FLS.1/RE	SF.SECURITY
FPT_TDC.1/RE	SF.ACCESS_CONTROL
FIA_ATD.1/AID	SF.ACCESS_CONTROL
FIA_UID.2/AID	SF.ACCESS_CONTROL
FIA_USB.1/AID	SF.ACCESS_CONTROL
FMT_MTD.1/JCRE	SF.ACCESS_CONTROL
FMT_MTD.3/JCRE	SF.ACCESS_CONTROL
FDP_ITC.2/Installer	SF.ACCESS_CONTROL
FMT_SMR.1/Installer	SF.ACCESS_CONTROL
FPT_FLS.1/Installer	SF.SECURITY
FPT_RCV.3.1/Installer	SF.TRANSACTION
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/CM	SF.SECURE_CHANNEL
FDP_IFC.2/CM	SF.SECURE_CHANNEL
FDP_IFF.1/CM	SF.SECURE_CHANNEL
FDP_UIT.1/CM	SF.SECURE_CHANNEL
FIA_UID.1/CM	SF.SECURE_CHANNEL
FMT_MSA.1/CM	SF.ACCESS_CONTROL
FMT_MSA.3/CM	SF.ACCESS_CONTROL
FMT_SMF.1/CM	SF.ACCESS_CONTROL
FMT_SMR.1/CM	SF.ACCESS_CONTROL
FTP_ITC.1/CM	SF.SECURE_CHANNEL
FTP_ITC.1/CCM	SF.SECURE_CHANNEL

7.10.3 Secure IC SFRs coverage

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

7.10.4 ITL SFRs coverage

Security Functional Requirement	**Coverage by TSS Security Function(s)**
FIA_UID.1/ITL	SF.ACCESS_CONTROL
FIA_UAU.1/ITL	SF.ACCESS_CONTROL

FIA_UAU.4/ITL	SF.ACCESS_CONTROL
FDP_IFC.2/ITL	SF.ACCESS_CONTROL
FDP_IFF.1/ITL	SF.ACCESS_CONTROL
FDP_RIP.1/ITL	SF.SECURITY
FMT_MSA.1/ITL	SF.ACCESS_CONTROL
FMT_MSA.3/ITL	SF.ACCESS_CONTROL
FMT_SMF.1/ITL	SF.ACCESS_CONTROL
FMT_SMR.1/ITL	SF.ACCESS_CONTROL
FPT_EMS.1/ITL	SF.SECURITY
FPT_FLS.1/ITL	SF.SECURITY
FTP_ITC.1/ITL	SF.SECURE_CHANNEL

7.10.5 Association table of SFRs and TSS

TSF	**SFR**
SF.TRANSACTION	FDP_ROL.1/FIREWALL FPT_RCV.3/Installer FDP_RIP.1/ABORT
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/eUICC

	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/PPR
	FMT_MSA.1/CERT_KEYS
	FMT_SMF.1/eUICC
	FMT_SMR.1/eUICC
	FMT_MSA.1/RAT
	FMT_MSA.3/eUICC
	FDP_ACC.2/FIREWALL
	FDP_ACF.1/FIREWALL
	FDP_IFC.1/JCVM
	FDP_IFF.1/JCVM
	FMT_MSA.1/JCRE
	FMT_MSA.1/JCVM
	FMT_MSA.2/FIREWALL_JCVM
	FMT_MSA.3/FIREWALL
	FMT_MSA.3/JCVM
	FDP_ITC.2/Installer
	FMT_SMR.1/Installer
	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/CM FMT_SMR.1/CM FMT_MSA.1/CM FMT_MSA.3/CM FMT_SMR.1/RE FMT_SMF.1/RE FPT_TDC.1/RE FIA_ATD.1/AID FIA_UID.2/AID FIA_USB.1/AID FMT_MTD.1/JCRE FMT_MTD.3/JCRE FMT_MSA.1/ITL FMT_MSA.3/ITL FIA_UID.1/ITL FIA_UAU.1/ITL FIA_UAU.4/ITL FDP_IFC.2/ITL FDP_IFF.1/ITL FMT_SMF.1/ITL FMT_SMR.1/ITL
SF.INTEGRITY	FDP_SDI.1/eUICC FDP_SDI.2/DATA
SF.SECURITY	FPT_FLS.1/Platform_services FPT_EMS.1/eUICC FDP_RIP.1/eUICC FPT_FLS.1/eUICC

	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/Installer FPT_FLS.1/ADEL FPT_FLS.1/ODEL FDP_RIP.1/ADEL FDP_RIP.1/ODEL FPT_PHP.3 FDP_RIP.1/ITL FPT_EMS.1/ITL FPT_FLS.1/ITL
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/CM FDP_IFC.2/CM

	FDP_IFF.1/CM FDP_UIT.1/CM FIA_UID.1/CM FTP_ITC.1/CCM FTP_ITC.1/CM FTP_ITC.1/ITL
SF.CRYPTO	FIA_API.1/eUICC FCS_CKM.1/SCP-SM FCS_CKM.2/SCP-MNO FCS_CKM.4/SCP-SM FCS_CKM.4/SCP-MNO FCS_COP.1/Mobile_network FCS_CKM.2/Mobile_network FCS_CKM.4/Mobile_network FCS_CKM.1/ECC FCS_CKM.1/Triple DES FCS_CKM.1/AES FCS_CKM.4/RE FCS_COP.1/SHA FCS_COP.1/SIG_ECC FCS_COP.1/MAC_TDES FCS_COP.1/MAC_AES FCS_COP.1/CIPH_TDES FCS_COP.1/CIPH_AES FCS_COP.1/CIPH_AES_GCM FCS_COP.1/ECKA-EG
SF.RNG	FCS_RNG.1
SF.IDENTITY	FIA_API.1/eUICC

	FAU_SAS.1

8. Statement of Compatibility

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

8.1 Classification of the Platform TSFs

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

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

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

Table 22 Classification of Platform-TSFs

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

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

8.2 Matching statement

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

- Certified microcontroller ST33K1M5C.
- True Random Number Generation with PTG.2 classification according to [AIS31].

- Cryptographic support based on symmetric key algorithms AES with 128, 192, 256 bits key length and Triple DES with 112, 168 bits key length.
- Cryptographic support based on asymmetric key algorithm ECDSA with up to 512 bits elliptic curve key length, including key generation.

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

8.3 Security objectives

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

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

The following platform objectives could be mapped to composite objectives:

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

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

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

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

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

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

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

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

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

8.4 Security objectives for the environment

Platform ST Sec. Obj. Env.	**Correspondence in Composite ST**	
	Relevant	TOE ST Sec. Objective
BSI.OE.Resp-Appl	Yes	O.KEY-MNGT, O.PIN-MNGT, O.TRANSACTION, O.OBJ-DE-LETION, O.DELETION, O.LOAD, O.INSTALL, O.API, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.ITL.SECURE_LOAD, O.ITL.CONFID_KEYS
BSI.OE.Process-Sec-IC	No	N/A
BSI.OE.Lim-Block-Loader	No	N/A
BSI.OE.Loader-Usage	No	N/A
BSI.OE.TOE-Auth	Yes	O.PPE-PPI, O.eUICC-DO-MAIN-RIGHTS
OE.Composite-TOE-Id	Yes	O.PROOF_OF_IDENTITY, O.TOE.IDENTIFICATION
OE.TOE-Id	Yes	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY
OE.Enable-Disable-Secure-Diag	No	N/A
OE.Secure-Diag-Usage	No	N/A

The table above shows the following:

- Column “Platform ST Sec. Obj. Env.” lists the Security Objectives for the Operational Environment from the Platform ST.

- Column “Relevant” specifies for each security objective if it is relevant for the composite certification or not.
- Column “TOE ST Sec. Objecitve” maps the security objectives for the TOE from Composite-ST to each relevant security objective for the operational environment from Platform-ST.

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

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

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

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

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

8.5 Security requirements

8.5.1 Security Functional Requirements

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

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

	FMT_MSA.1/RAT, FMT_MSA.1/CERT_KEYS, FMT_MSA.1/PPR, FMT_MSA.1/PLAT-FORM_DATA, FMT_MSA.1/ITL
FMT_MSA.3 / Memories	FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MSA.3/ADEL, FMT_MSA.3/CM, FMT_MSA.3, FMT_MSA.3/ITL
FMT_SMF.1 / Memories	FMT_SMF.1, FMT_SMF.1/ADEL, FMT_SMF.1/CM
FIA_API.1	Nor relevant, since the TOE is delivered in User configuration.
FTP_ITC.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_UCT.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_UIT.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_ACC.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FDP_ACF.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_MSA.3 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_MSA.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.
FMT_SMR.1 / Loader	Not relevant, since the Flash Loader is permanently deactivated.

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

8.5.2 Security Assurance Requirements

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

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

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

9. References

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

[AGD_PRE] Preparative Procedures for Sm@rtSIM Polaris SGP.22 (confidential document), Version 1.0, 26.06.2024

[AGD_OPE] Sm@rtSIM Next Generation v1.0 Personalization Guide (confidential document), Version 1.1.1, 02.05.2024

Sm@rtSIM Polaris SGP.22, API Support (confidential document), Version 0.2, 06.07.2023

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

[AGD_SEC] Security Guidance for Sm@rtSIM Polaris SGP.22 (confidential document), Version 1.1, 20.03.2024

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

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

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

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

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

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 5, April 2017. CCMB-2017-04-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 5, April 2017. CCMB-2017-04-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components. Version 3.1, Revision 5, April 2017. CCMB-2017-04-003.

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

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

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

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

[GP] GlobalPlatform Card Specification, Version 2.3.1

[GP AM B] GlobalPlatform Card Specification v2.2 Amendment B – Remote Application Management over HTTP, Version 1.1.3, May 2015.

[GP AM D] GlobalPlatform Card Specification v2.2 Amendment D – Secure Channel Protocol 03, Version 1.1.1

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

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

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

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

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

[ISO 9797-1] ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1:

Mechanisms using a block cipher.

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

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

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

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

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

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

[JIL] Certification of “open” smart card products, Version 1.1 (for trial use), 4 February 2013, Joint Interpretation Library.

[JVM] The Java Virtual Machine Specification. Lindholm, Yellin. ISBN 0-201-43294-3.

[KS2011] W. Killmann, W.Schindler, A proposal for: Functionality classes for random number generators, version 2.0, September 2011.

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

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

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

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

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

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

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

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

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

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

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

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

[SGP.21] Remote SIM Provisioning (RSP) Architecture, version 2.4, GMSA Association, 03 August 2021.

[SGP.22] RSP Technical Specification, GSM Association, Version 2.4, 28 October 2021.

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

[PP-eUICC] Embedded UICC for Consumer Devices Protection Profile, GSM Association, Version 1.0 05-June-2018.

[SIMalliance] SIMalliance eUICC Profile Package: Interoperable Format Technical Specification V2.1.

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

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

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

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

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

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

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

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

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

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

[IC_ST] ST33K1M5C and ST33K1M5T C01 Security Target for composition, SMD_ST33K1M5_ST_21_001 Rev C01.1, May 2023, STMicroelectronics.

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

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

dci

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

[GDIMS] Certification Report CCN-CC/2022-01/INF-3825 for Giesecke+Devrient Development Center Spain (GDIMS), related to CCN-CC-23/2022, 26 May 2022 (Certificate Date), National Cryptologic Centre (CCN). https://oc.ccn.cni.es/productos-certificados/centros-certificados/622-ganddvriberica-gdims

[NAN] Certification Report CCN-CC/2023-26/INF-4297 for Giesecke+Devrient (China) Technologies GDCNMS NAN, related to CCN-CC-6/2024, 22 March 2024 (Certificate Date), National Cryptologic Centre (CCN). https://oc.ccn.cni.es/productos-certificados/centros-certificados/1011-giesecke-devrient-jiangxi-technology-co-ltd-gdcnms-nan

List of tables

Table 1 TOE life-cycle phases and TOE delivery..... 9
Table 2 Assets Consistency 15
Table 3 Users consistency 15
Table 4 Subjects Consistency 16
Table 5 Threats Consistency.....18
Table 6 Organizational Security Policies Consistency 18
Table 7 Assumptions Consistency.....18
Table 8 Security objectives for the TOE consistency 21
Table 9 Security Objectives for the Operational Environment Consistency..22
Table 10 Security Functional Requirement Consistency.....29
Table 11 Refined Threats.....32
Table 12 Threats and Security Objectives Coverage.....43
Table 13 Security Objectives and Threats – Coverage.....45
Table 14 OSPs and Security Objectives – Coverage.....45
Table 15 Security Objectives and OSPs – Coverage.....47
Table 16 Assumptions and Security Objectives for the Operational Environment - Coverage.....47
Table 17 Security Objectives for the Operational Environment and Assumptions – Coverage 48
Table 18 SFRs of the TOE of this ST 50
Table 19 Extension of SFR Dependencies 86
Table 20 IC Security Objectives and SFRs – Coverage.....88
Table 21 ITL Security Objectives and SFRs – Coverage 90
Table 22 Classification of Platform-TSFs.....113