Security Target Lite of iSIM v4.0

D1570537, Release 1.0p, January 2023

Security Target

REVISION HISTORY

Ver	Date	Description of the modifications
1.0p	19/01/2023	Official release

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

All the information provided in this document is provided based on our best knowledge and may change over the time to reflect evolution and/or modification of product features and characteristics.

Thales DIS, its affiliate and representatives accept no duty of care nor liability of any kind whatsoever to any third party, and no responsibility for damages, if any, suffered by any third party as a result of decisions made, or not made, or actions taken, or not taken, based on this document.

Product is certified including preparation, user and administration guidance.

Such guidance defines recommendations explaining how to fulfill security objectives for environment as defined in TOE.

Thales DIS highly recommends following such guidance for secure product deployment.

It is up to the risk manager to check or to rely on evidences that guidance are applied by relevant actors.

Thales DIS will not be held responsible for non-implementation of recommendations and associated consequences.

1 ST INTRODUCTION

1.1 ST reference

The ST identification is the following:

Title:	Security Target Lite of iSIM v4.0
Version:	1.0p
Author:	Thales
Reference:	D1570537
Publication date:	19/01/2023

1.2 TOE reference

Product name:	iSIM v4.0
Developer:	Thales
TOE name:	iSIM v4.0
TOE version:	61E800 (EUICCInfo2)
TOE documentation:	Guidance **[GUIDES]**
TOE hardware part:	SPU270 embedded in SM8550 SoC

2 TOE OVERVIEW

2.1 TOE description

The product **iSIM v4.0** is an Integrated eUICC (ieUICC) for Consumer Devices.

It is composed of:

- An Integrated Tamper Resistant Element (I-TRE): hardware sub-system withing a System-on-Chip (SoC) and its low-level kernel and software services
- The Integrated eUICC OS: software executed inside the I-TRE hardware, is stored securely in the I-TRE internal memories and/or in remote memories, typically the hosting device Non Volatile Memory and/or RAM

The TOE is the **Integrated eUICC** open platform with multi-application support, such as Java Card, GlobalPlatform, that implements the GSMA Remote SIM Provisioning (RSP) Architecture for Consumer Devices compliant with the GSMA specifications **[SGP.21] [SGP.22] [SGP.23]** and the Trusted Connectivity Alliance eUICC Profile Package implementing **[EUPP].**

2.1.1   TOE type and usage

The TOE type is software.

The ieUICC is an UICC embedded in a consumer device. The ieUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile.
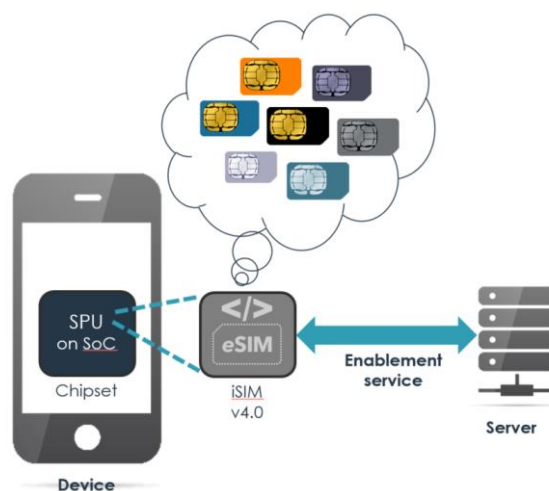
Figure 1 – Product environment

The TOE relies on a Local Profile Assistant (LPA) component. It can be either be implemented at the application level as LPAe (the case covered by the LPA PP-Module), or it can be implemented as a non-TOE on-device unit called LPAd. In this product, **the LPAe is not in the TOE**.

The **OS update** capability is available to correct existing features as required by the GSMA specifications.

The **Profiles are not part of the TOE**.

Figure 2 can represent the architecture overview of the **iSIM v4.0** and its decomposition in three layers: the I-TRE, the iSIM operating system and the iSIM data.
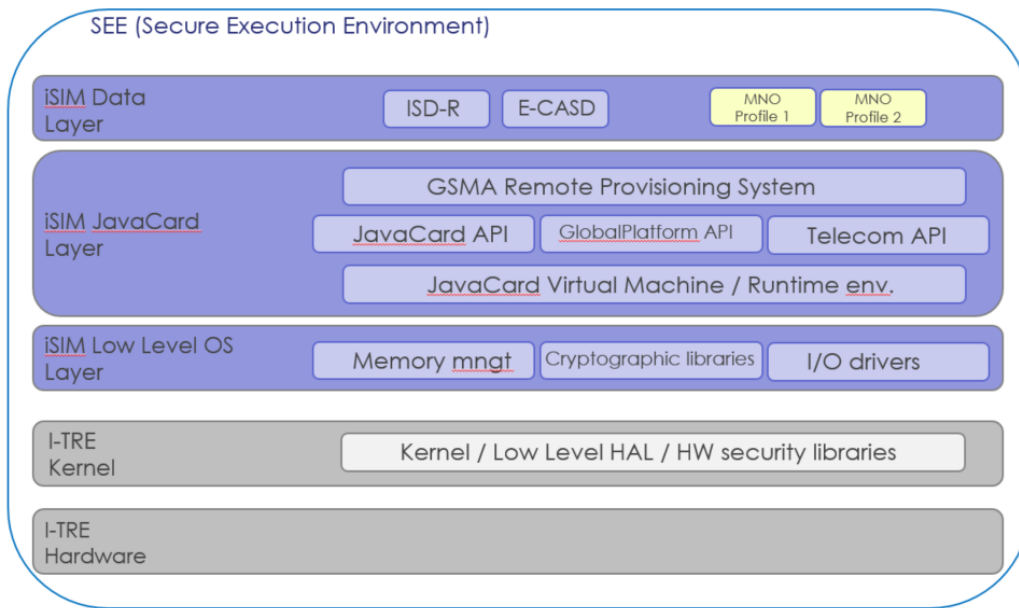
Figure 2 – iSIM v4.0 overview

Figure 3 can represent the architecture decomposition of the **iSIM v4.0** product. The elements in blue are related to Thales iSIM while the elements in red are related to I-TRE.
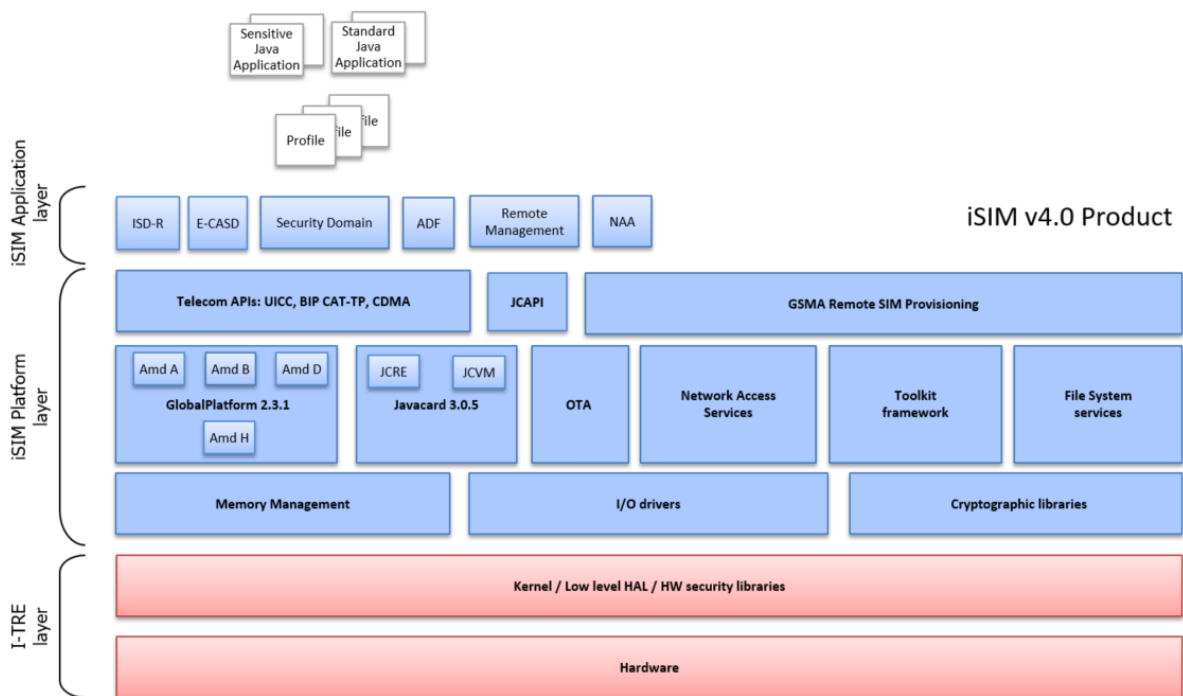
Figure 3 – iSIM v4.0 architecture

The TOE includes:

- the I-TRE layer providing support to the platform layer
- the iSIM platform layer composed of set of functions providing support to the application layer
- the iSIM application layer composed of privileged applications providing the remote provisioning and administration functionnality

2.1.2 TOE life-cycle

The product and TOE lice-cycle is composed of 5 phases (from phase a to e) which are described in Figure 4, in Table 1 and Table 2 with the mention of actors involved in each phase, as well as the associated locations. The TOE delivery is mentioned (dash line in red) before phase d.
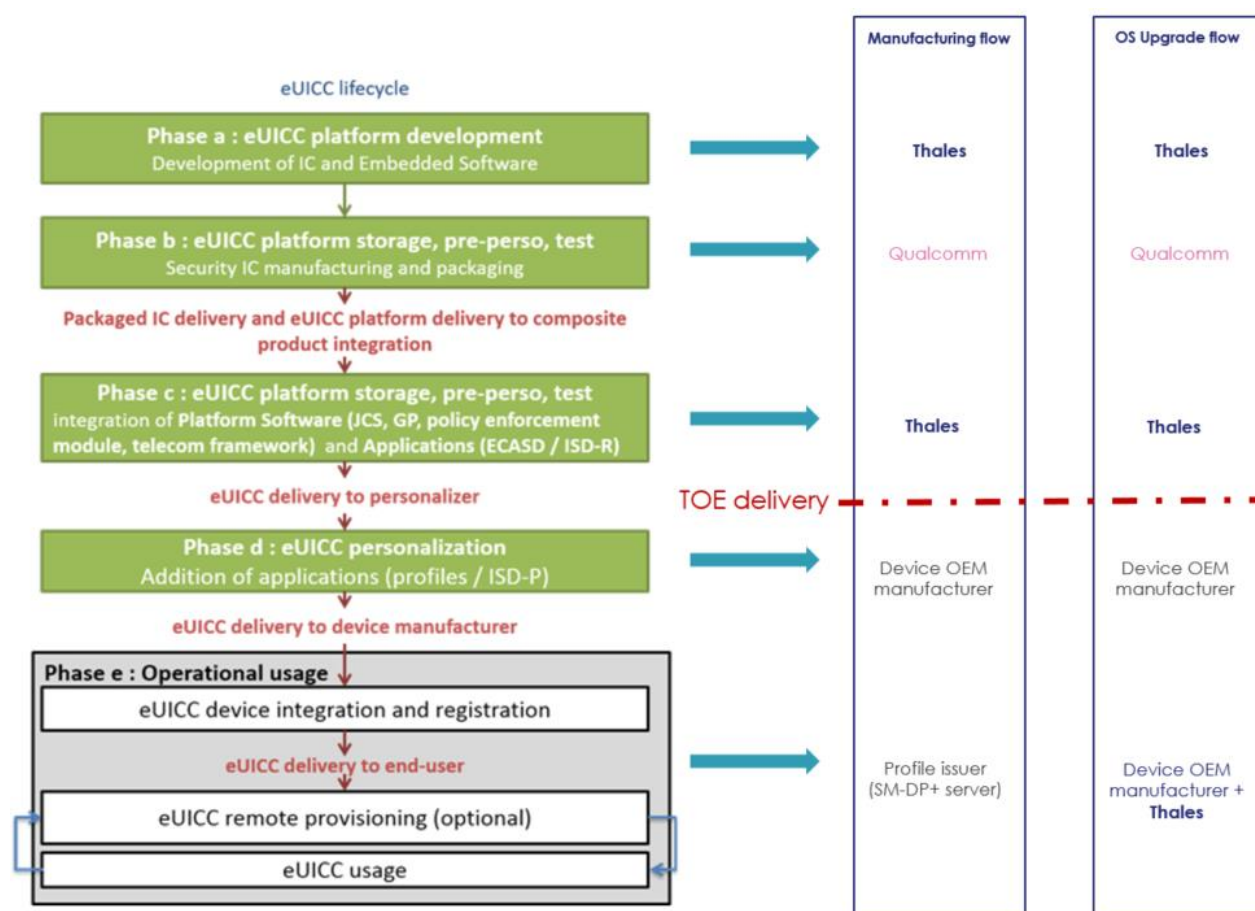
Figure 4 – TOE life-cycle and actors

The actors:

- The eUICC Manufacturer (EUM) is the developer of the ieUICC secure application (Thales).
- The I-TRE manufacturer is the developer and manufacturer of the I-TRE (Qualcomm).
- The Device OEM manufacturer is the Original Equipment Manufacturer.
- The Profile issuer is MNO that has privilege through its OTA Server to perform Remote Card Content Management (CCM) operations within its own profile (ISD-P). And, through its RSP servers, it also can provide Profiles to the end user, but has no privileges to manage profiles remotely without end user consent.
- The Application Providers (AP) are entities or institutions responsible for their applications and associated services. It may be for example a financial institution (a bank) or a transport operator.

- The End User is the user of the device and the ieUICC secure application represented with.

In the next tables, the * means that it is in secure environment and sites are covered by CC/EMVCo or GSMA SAS-UP site audit.

The manufacturing flow is described in the following table:

Phase	Description	Actor	Location
a	ieUICC Secure Application (iSIM OS) development / Validation	Thales*	Meudon (France)
b	I-TRE SoC manufacturing, test and sensitive assets management (Root Of Trust) • SAS UP – Perso_SC (2-step personalization – see chapter 11 FS.17 & FS.18)	Qualcomm*	• Amkor Korea (K3) • SPILZK (Taiwan)
Phase a and b steps are combined to prepare phase c where ieUICC Secure Application (iSIM OS) is generated with confidentiality and integrity thanks to re-use of Perso-SC Root of Trust assets			
c	ieUICC Secure Application (iSIM OS static image) image build and data generation (secure dynamic images)		
	Product Engineering • iSIM OS static image ciphering and signing using Thales TrustCenter (ciphering/transciphering service hosted in KMS through Thales secure room)	Thales*	Gemenos (France)
	Factory enablement • SAS UP – Perso_UICC (2-step personalization – see chapter 11 FS.17 & FS.18)	Thales*	Pont Audemer (France)
	Data Center – Remote Activation Server • SAS UP – Perso_UICC (2-step personalization – see chapter 11 FS.17 & FS.18)	Thales*	Tours (France)
*** TOE delivery *** *Static and dynamic images are securely (phase c images are ciphered and signed using phase b Root of Trusts) delivered to Phase d. In addition, transfer from phase c to phase d is managed with additional transport ciphering thanks to SSH keys used by transfer server (Allynis Connect)*			
d	ieUICC Secure Application (iSIM OS) and generic personalization loading + enablement of ieUICC (optional) Secure Application during device manufacturing and test flow	Device OEM manufacturer	Device OEM manufacturing premises
Device is delivered to point of sales and is reaching end user			
e	enablement of ieUICC (optional if not done at phase d) + RSP process (Profile loading and activation)	Profile issuer (SM-DP+ server)	In the field Remote access by end user to server associated to MNO / Carrier

Table 1 – TOE life-cycle (manufacturing flow)

The OS upgrade flow is described in the following table:

The conditions to trigger OS upgrade are weakness on ieUICC Secure Application (iSIM OS) at security, or functional, or both –OR– deployment of additional feature.

Phase	Description	Actor	Location
a	ieUICC Secure Application (iSIM OS) upgrade development / Validation	Thales*	Meudon (France)
b	I-TRE SoC manufacturing, test and sensitive assets management (Root Of Trust) • SAS UP – Perso_SC (2-step personalization – see chapter 11 FS.17 & FS.18)	Qualcomm*	• Amkor Korea (K3) • SPILZK (Taiwan)
	Phase a and b steps are combined to prepare phase c where ieUICC Secure Application (iSIM OS) is generated with confidentiality and integrity thanks to re-use of Perso-SC Root of Trust assets		
c	ieUICC Secure Application (iSIM OS static image) image build and data generation (secure dynamic images)		
	Product Engineering • iSIM OS static image ciphering and signing using Thales TrustCenter (ciphering/transciphering service hosted in KMS through Thales secure room)	Thales*	Gemenos (France)
	Factory enablement • SAS UP – Perso_UICC (2-step personalization – see chapter 11 FS.17 & FS.18)	Thales*	Pont Audemer (France)
	Data Center – Remote Activation Server • SAS UP – Perso_UICC (2-step personalization – see chapter 11 FS.17 & FS.18)	Thales*	Tours (France)
	*** TOE delivery *** *Static and dynamic images are securely (phase c images are ciphered and signed using phase b Root of Trusts) delivered to Phase d. In addition, transfer from phase c to phase d is managed with additional transport ciphering thanks to SSH keys used by transfer server (Allynis Connect)*		
d	Upgraded ieUICC Secure Application (iSIM OS) and generic personalization delivery	Device OEM manufacturer	Device OEM manufacturing premises
	Upgraded ieUICC Secure Application (iSIM OS) will be send over the air to already deployed devices		
e	Loading enablement of ieUICC (optional if not done at phase d) • Data Center – Remote Activation Server SAS UP – Perso_UICC (2-step personalization – see chapter 11 FS.17 & FS.18)	Device OEM manufacturer + Thales*	In the field Remote access to device manufacturer server + Tours (France)

Table 2 – TOE life-cycle (OS upgrade flow)

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

Non-TOE is same than the ones mentioned in the [PP-EUICC].
The TOE does not implement the RMI functions from JCS.

2.2 TOE scope

2.2.1 Physical scope

Figure 5 – TOE physical boundaries

The physical boundaries encompass the iSIM software executed inside the I-TRE hardware. The other items are outside the scope of the evaluation as illustrated in Figure 5.

2.2.2 Logical scope

The logical boundaries are delimited (dash line in red) in Figure 6.
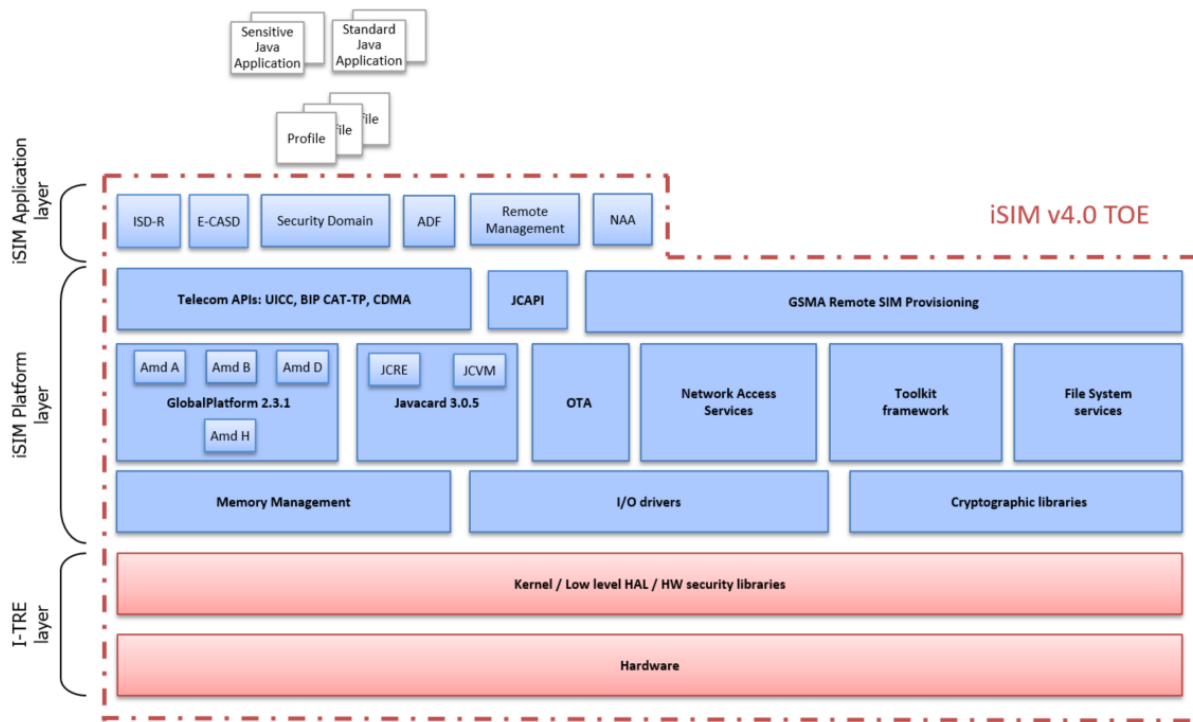
Figure 6 – TOE logical boundaries

The TOE consists of the following components:

TOE component	Developer	Item	Identifier	Form of delivery	Certification identifier
Integrated TRE (I-TRE)	Qualcomm	SPU hard macro embedded in SM8550 SoC	6.1	Bare die	CC-23-0569293
	Qualcomm	SPU ROM code	77100000	Firmware	
	Qualcomm	SPU MCP image	SPSS.A1.1.7-00071-KAILUA-1	Software	
	Qualcomm	SPU guidances	[GUIDES/I-TRE]	Document	
Integrated eUICC OS	Thales	iSIM v4.0	61E800	Software	THIS
Integrated eUICC guidances	Thales	iSIM v4.0	[GUIDES]	Document	THIS

Table 3 – TOE components

The Integrated eUICC OS implements (at least) the following services:

- Enablement Service and Remote Sim Provisioning
- Management and control of the communication between OS and external entities
- OS Security services as:
  - providing secure cryptographic primitives, algorithms and servives
  - ensure the security of assets
  - generating random numbers
- Enforcement of the Javacard Runtime and Firewall mechanism
- Standard APIs such as Telecom APIs, JC APIs and GP APIs

3 CONFORMANCE CLAIMS

Evaluation type:

- This is a composite evaluation, which relies on the SPU270 embedded in SM8550 SoC certificate and evaluation results.

  ▪ Certification done under the NSCIB scheme

  ▪ Certificate : NSCIB-0569293

  ▪ Security Target **[ST/ITRE]** conformance to **[PP-84]** and **[SGP.08]** as required by the GSM Association (GSMA) for Integrated eUICC

  ▪ CC version: 3.1, revision 5

  ▪ Assurance level: EAL4+ (ALC_DVS.2 and AVA_VAN.5 augmentations)

The composite evaluation includes the additional composition tasks defined in the [CC-COMP].

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

This Security Target conforms to CC version 3.1 release 5 [CC-1], [CC-2] and [CC-3].

This Security Target is CC Part 2 [CC-2] extended and CC Part 3 [CC-3] conformant of Common Criteria version 3.1, revision 5.

3.2 Assurance package

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

3.3 Protection Profile (PP) conformance claim

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

3.4 Conformance claim rationale

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

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

3.4.1   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] when the embedded eUICC is embedded in a certified IC, but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs in order to meet the objectives for the OS and JCS. This is a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

3.4.2   SPD Consistency

3.4.2.1   Assets consistency

All assets defined in [PP-eUICC] are relevant for the TOE of this Security Target. The table below indicates the assets' consistency and the additions from [PP-JCS].

Assets	PP-eUICC	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_POLICY_RULES	X	(E)
D.PROFILE_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_CODE		(A): Added from [PP-JCS].
D.APP_C_DATA		(A): Added from [PP-JCS].
D.APP_I_DATA		(A): Added from [PP-JCS].
D.APP_KEYs		(A): Added from [PP-JCS].
D.PIN		(A): Added from [PP-JCS].
D.API_DATA		(A): Added from [PP-JCS].
D.CRYPTO		(A): Added from [PP-JCS].
D.JCS_CODE		(A): Added from [PP-JCS].
D.JCS_DATA		(A): Added from [PP-JCS].
D.SEC_DATA		(A): Added from [PP-JCS].

Table 4 - Assets Consistency table

3.4.2.2 Users and Subjects consistency

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

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

Table 5 - User consistency table

All Subjects defined in [PP-eUICC] are relevant for the TOE of this Security Target. The table below indicates the Subjects' consistency and the additions from [PP-JCS].

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.PACKAGE		(A): Added from [PP-JCS].

Table 6 - Subjects Consistency table

3.4.2.3 Threats consistency

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

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

Threats	PP-eUICC	Security Target
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)
T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)

Table 7 - Threats Consistency table

3.4.2.4   Organizational Security Policies consistency

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

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

Table 8 - Organizational Security Policies Consistency table

3.4.2.5   Assumptions consistency

All Assumptions defined in [PP-eUICC] are relevant for the TOE of this Security Target. The table below indicates the Assumptions consistency.

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

Table 9 - Assumptions Consistency table

3.4.3   Security Objectives Consistency

3.4.3.1   Objective for the TOE consistency

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

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

O.TOE	PP-eUICC	Security Target
O.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.TOE	PP-eUICC	Security Target
O.IC.PROOF_OF IDENTITY		(A): Added and replace OE.IC.PROOF_OF IDENTITY from [PP-eUICC].
O.IC.SUPPORT		Added and replace OE.IC.SUPPORT from [PP-eUICC].
O.IC.RECOVERY		(A): Added and replace OE.IC.RECOVERY from [PP-eUICC].
O.RE.PPE-PPI		(A): Added and replace OE.RE.PPE-PPI from [PP-eUICC].
O.RE.SECURE-COMM		Added and replace OE.RE.SECURE-COMM from [PP-eUICC].
O.RE.API		(A): Added and replace OE.RE.API from [PP-eUICC].
O.RE.DATA-CONFIDENTIALITY		(A): Added and replace OE.RE.DATA-CONFIDENTIALITY from [PP-eUICC].
O.RE.DATA-INTEGRITY		(A): Added and replace OE.RE.DATA-INTEGRITY from [PP-eUICC].
O.RE.IDENTITY		(A): Added and replace OE.RE.IDENTITY from [PP-eUICC].
O.RE.CODE-EXE		(A): Added and replace OE.RE.CODE-EXE from [PP-eUICC].

Table 10 - Security objectives for the TOE consistency table

3.4.3.2 Objective for Environment consistency

O.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-DPplus	X	(E)
OE.MNO	X	(E)
OE.TRUSTED-PATHS-LPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.CODE-EVIDENCE	X	(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-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE

Table 11 - Security objectives for the Operational Environment consistency table

3.4.4 Conformity of the Requirement (SFR/SAR)

3.4.4.1 SFR consistency

SFR	PP-eUICC	Security Target
FIA_UID.1/EXT	X	
FIA_UAU.1/EXT	X	
FIA_USB.1/EXT	X	
FIA_UAU.4/EXT	X	
FIA_UID.1/MNO-SD	X	
FIA_USB.1/MNO-SD	X	
FIA_ATD.1	X	
FIA_API.1	X	
FDP_IFC.1/SCP	X	
FDP_IFF.1/SCP	X	
FTP_ITC.1/SCP	X	
FDP_ITC.2/SCP	X	
FPT_TDC.1/SCP	X	
FDP_UCT.1/SCP	X	
FDP_UIT.1/SCP	X	
FCS_CKM.1/SCP-SM	X	
FCS_CKM.2/SCP-MNO	X	
FCS_CKM.4/SCP-SM	X	
FCS_CKM.4/SCP-MNO	X	
FDP_ACC.1/ISDR	X	
FDP_ACF.1/ISDR	X	
FDP_ACC.1/ECASD	X	
FDP_ACF.1/ECASD	X	
FDP_IFC.1/Platform_services	X	
FDP_IFF.1/Platform_services	X	
FPT_FLS.1/Platform_services	X	
FCS_RNG.1	X	
FPT_EMS.1	X	
FDP_SDI.1	X	
FDP_RIP.1	X	
FPT_FLS.1	X	
FMT_MSA.1/PLATFORM_DATA	X	
FMT_MSA.1/PPR	X	
FMT_MSA.1/CERT_KEYS	X	
FMT_SMF.1	X	
FMT_SMR.1	X	
FMT_MSA.1/RAT	X	
FMT_MSA.3	X	
FCS_COP.1/Mobile_network	X	
FCS_CKM.2/Mobile_network	X	
FCS_CKM.4/Mobile_network	X	
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].

SFR	PP-eUICC	Security Target
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/JC		(A): Added from [PP-JCS]. Refined with iteration.
FMT_SMR.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/RSA FCS_CKM.1/EC		(A): Added from [PP-JCS]. Refined with iteration. (A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/GP-SCP		(A): Added from [PP-GP].
FCS_CKM.4		(A): Added from [PP-JCS].
FCS_COP.1/TDES_MAC FCS_COP.1/AES_MAC FCS_COP.1/ECDH FCS_COP.1/CRC FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_COP.1/GP-SCP FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/RSA_SIGN FCS_COP.1/RSA_CIPHER FCS_COP.1/Hash FCS_COP.1/HMAC		(A): Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A): Added from [PP-JCS].
FDP_RIP.1/APDU		(A): Added from [PP-JCS].
FDP_RIP.1/bArray		(A): Added from [PP-JCS].
FDP_RIP.1/GlobalArray		(A): Added from [PP-JCS].
FDP_RIP.1/KEYS		(A): Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A): Added from [PP-JCS].
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/JC		(A): Added from [PP-JCS]. Refined with iteration.
FPT_TDC.1		(A): Added from [PP-JCS].
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].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].

SFR	PP-eUICC	Security Target
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].
FTP_ITC.1/CM		(A): Added from [PP-JCS].
FPT_FLS.1/GP		(A): Added from [PP-GP].
FDP_ROL.1/GP		(A): Added from [PP-GP].
FCO_NRO.2/GP		(A): Added from [PP-GP].
FMT_SMR.1/GP		(A): Added from [PP-GP].
FMT_SMF.1/GP		(A): Added from [PP-GP].
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP].
FDP_ITC.2/GP-KL		(A): Added from [PP-GP].
FPT_RCV.3/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP].
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP].
FIA_UID.1/GP		(A): Added from [PP-GP].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FTP_ITC.1/GP		(A): Added from [PP-GP].
FPR_UNO.1/GP		(A): Added from [PP-GP].
FPT_TDC.1/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-KL		(A): Added from [PP-GP].
FDP_IFF.1/GP-KL		(A): Added from [PP-GP].
FMT_MSA.1/GP		(A): Added from [PP-GP].
FMT_MSA.3/GP		(A): Added from [PP-GP].
FAU_SAS.1		(A): Added to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added to cover O.IC.RECOVERY.
FPT_RCV.4/OS		(A): Added to cover O.IC.SUPPORT.

Table 12 - Security Functional Requirement consistency table

3.4.4.2   SAR consistency

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

4 SECURITY PROBLEM DEFINITION

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

4.1 Assets

The definition of the assets from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.1 for complete list is assets.

Assets
D.MNO_KEYS
D.PROFILE_NAA_PARAMS
D.PROFILE_IDENTITY
D.PROFILE_POLICY_RULES
D.PROFILE_USER_CODES
D.PROFILE_CODE
D.TSF_CODE
D.PLATFORM_DATA
D.DEVICE_INFO
D.PLATFORM_RAT
D.SK.EUICC.ECDSA
D.CERT.EUICC.ECDSA
D.PK.CI.ECDSA
D.EID
D.SECRETS
D.CERT.EUM.ECDSA
D.CRLs
D.APP_CODE
D.APP_C_DATA
D.APP_I_DATA
D.APP_KEYs
D.PIN
D.API_DATA
D.CRYPTO
D.JCS_CODE
D.JCS_DATA
D.SEC_DATA

4.2 Users and Subjects

The definition of users and subjects from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.2 for complete list is users and subjects.

User
U.SM-DPplus
U.MNO-OTA
U.MNO-SD

Subjects
S.ISD-R
S.ISD-P
S.ECASD
S.PPI
S.PPE
S.TELECOM
S.ADEL
S.APPLET
S.BCV
S.CAD
S.INSTALLER
S.JCRE
S.JCVM
S.LOCAL
S.MEMBER
S.PACKAGE

4.3 Threats

The definition of threats from [PP-eUICC] where no refinements are made is not repeated here. See section 3.4.2.3 for complete list is threats.

Threats	Refined threats description
T.UNAUTHORIZED-PROFILE-MNG	Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, **D.APP_C_DATA, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_CODE**.
T.UNAUTHORIZED-PLATFORM-MNG	Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behaviour of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.
T.PROFILE-MNG-INTERCEPTION	Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, **D.APP_C_DATA, D.PIN and D.APP_KEYs**.
T.PROFILE-MNG-ELIGIBILITY	Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, **D.APP_C_DATA, D.PIN, D.APP_KEYs, D.APP_CODE and D.APP_I_DATA**.
T.UNAUTHORIZED-IDENTITY-MNG	Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs., **D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA**.
T.IDENTITY-INTERCEPTION	Directly threatens the assets: D.SECRETS, D.EID, **D.APP_C_DATA, D.PIN and D.APP_KEYs**.
T.UNAUTHORIZED-eUICC	
T.LPAd-INTERFACE-EXPLOIT	
T.UNAUTHORIZED-MOBILE-ACCESS	

Threats	Refined threats description
T.LOGICAL-ATTACK	Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_POLICY_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, **D.JCS_CODE, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_C_DATA**.
T.PHYSICAL-ATTACK	

4.4 Organizational Security Policies

The definition of organizational security policies from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.4 for complete list is organizational security policies.

OSPs
OSP.LIFE-CYCLE

5 SECURITY OBJECTIVES

This section introduces the security objectives for the TOE.

5.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 3.4.3 for complete list is Security Objectives for the TOE.

Some objectives from the environment have been converted to objectives of the TOE, specifically the ones from [PP-eUICC] related to OE.RE* and OE.IC*. The replaced objectives from 3.4.3.2 and their description are listed next:

O.TOE	Replaced objectives description
O.PPE-PPI	
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
O.IC.PROOF_OF IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: (1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification). (2) It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PPE, S.PPI, and S.TELECOM). (3) It allows the S.PPE, S.PPI, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection). (4) It provides a means to perform memory operations atomically for S.PPE, S.PPI, and S.TELECOM.

O.TOE	Replaced objectives description
O.IC.RECOVERY	If there is a loss of power while an operation is in progress, the underlying IC must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.
O.RE.PPE-PPI	The Runtime Environment shall provide secure means for card management activities, including: o load of a package file, o installation of a package file, o extradition of a package file or an application, o personalization of an application or a Security Domain, o deletion of a package file or an application, o privileges update of an application or a Security Domain, o access to an application outside of its expected availability.
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.
O.RE.API	The Runtime Environment shall ensure that native code can be invoked only via an API.
O.RE.DATA-CONFIDENTIALITY	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
O.RE.IDENTITY	The Runtime Environment shall ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.

5.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 3.4.3.2 for complete list is Security Objectives for the Operational Environment.

O.ENV
OE.CI
OE.SM-DPplus
OE.MNO
OE.TRUSTED-PATHS-LPAd
OE.APPLICATIONS
OE.CODE-EVIDENCE
OE.MNO-SD

5.3 Security Objectives Rationale

5.3.1 Threats

5.3.1.1 *Unauthorized profile and platform management*

T.UNAUTHORIZED-PROFILE-MNG:

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

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

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

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

T.UNAUTHORIZED-PLATFORM-MNG

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

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

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.

5.3.1.2 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.

5.3.1.3 eUICC cloning

T.UNAUTHORIZED-eUICC

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

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

5.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

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

5.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS

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

5.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

- by the APIs provided by the Runtime Environment (O.RE.API);
- by the APIs of the TSF (O.API); the APIs of Telecom Framework, 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).

This threat is covered by:
- prevention of unauthorized code execution by applications (O.RE.CODE-EXE).

The following objectives for the operational environment are also required:

- 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).

5.3.2 Organizational Security Policies

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

OSPs
OSP.LIFE-CYCLE

5.3.3 Assumptions

The assumptions A.TRUSTED-PATHS-LPAd, A.ACTORS and A.APPLICATIONS are defined as in [PP-eUICC].

Assumptions
A.TRUSTED-PATHS-LPAd
A.ACTORS
A.APPLICATIONS

5.3.4 Rationale tables

5.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZEDPROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DPplus, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Section 5.3.1.1
T.UNAUTHORIZEDPLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 5.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DPplus, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD	Section 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DPplus, O.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 5.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 5.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	Section 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 5.3.1.5

Threats	Security Objectives	Rationale
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 5.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 5.3.1.6

Table 13 - 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.UNAUTHORIZED-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 |

Table 14 - Security Objectives and threats

5.3.4.2 Organizational Security Policies Rationale

Organizational Security Policies	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PPE-PPI, O.RE.PPE-PPI, O.OPERATE	Section 5.1

Table 15 - Organizational Security Policies and Security Objectives- Coverage

Security Objectives	Organizational 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.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	
OE.SM-DS	

Table 16 - Security Objectives and Organizational Security Policies

5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale

A.TRUSTED-PATHS-LPAd	OE.TRUSTED-PATHS-LPAd	Section 5.3.3
A.ACTORS	OE.CI, OE.SM-DPplus, OE.MNO	Section 5.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	Section 5.3.3

Table 17 - 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.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PPE-PPI	
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.MNO-SD	

Table 18 - Assumptions and Security Objectives for the Operational Environment

6 EXTENDED COMPONENTS DEFINITION

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-84], section 5.3 have been taken with no modification.

7 SECURITY REQUIREMENTS

The following conventions are used in the definitions of the SFRs:
- Selections and assignments that have already been made in the [PP-eUICC] are in **bold**, and the original text on which the selection or assignment has been made is not reminded.
- Selections and assignments made in this ST are in blue or **bold blue**.

7.1 eUICC Security Functional Requirements

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

7.1.1 Identification and authentication

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow

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

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

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

FIA_UAU.1/EXT Timing of authentication

FIA_UAU.1.1/EXT The TSF shall allow

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

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

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

FIA_USB.1/EXT User-subject binding

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

     ○ **SM-DP+ OID is associated to S.ISD-R, acting on behalf of U.SM-DPplus**

     ○ **MNO OID is associated to U.MNO-SD, acting on behalf of U.MNO-OTA**.

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

     ○ **Initial association of SM-DP+ OID and MNO OID requires U.SM-DPplus to be authenticated via "CERT.DPauth.ECDSA"**.

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

     ○ **change of SM-DP+ OID requires U.SM-DPplus to be authenticated via "CERT.DPauth.ECDSA"**

     ○ **change of MNO OID is not allowed**.

FIA_UAU.4/EXT Single-use authentication mechanisms

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

     ○ **U.SM-DPplus**

     ○ **U.MNO-OTA**.

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow [assignment: list of none] on behalf of the user to be performed before the user is identified.

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

FIA_USB.1/MNO-SD User-subject binding

FIA_USB.1.1/MNO-SD The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **The U.MNO-SD AID is associated to the S.ISD-P acting on behalf of U.MNO-SD**.

FIA_USB.1.2/MNO-SD The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **Initial association of AID requires U.SM-DP+ to be authenticated via CERT.DPauth.ECDSA**.

FIA_USB.1.3/MNO-SD The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **no change of AID is allowed**.

FIA_ATD.1 User attribute definition

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

- o **CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-DPplus;**
- o **MNO OID belonging to U.MNO-OTA;**
- o **AID belonging to U.MNO-SD.**

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **cryptographic authentication mechanism based on the EID of the eUICC** to prove the identity of the TOE to an external entity.

7.1.2 Communication

FDP_IFC.1/SCP Subset information flow control

FDP_IFC.1.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** on

- o **users/subjects:**
  - ▪ **U.SM-DPplus and S.ISD-R**
  - ▪ **U.MNO-OTA and U.MNO-SD**
- o **information: transmission of commands.**

FDP_IFF.1/SCP Simple security attributes

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

- o **users/subjects:**
  - ▪ **U.SM-DPplus and S.ISD-R, with security attribute D.SECRETS**
  - ▪ **U.MNO-OTA and U.MNO-SD, with security attribute D.MNO_KEYS**
- o **information: transmission of commands**.

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

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

FDP_IFF.1.3/SCP The TSF shall enforce the [assignment: none].

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

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

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

FTP_ITC.1/SCP Inter-TSF trusted channel

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

FTP_ITC.1.2/SCP The TSF shall permit <u>another trusted IT product</u> to initiate communication via the trusted channel.

FTP_ITC.1.3/SCP The TSF shall initiate communication via the trusted channel for [assignment: following list of functions for which a trusted channel is required].

The TSF shall permit the SM-DP+ to open a SCP-SGP22 secure channel to transmit the following operations:

- ES8+.InitialiseSecureChannel
- ES8+.ConfigureISDP
- ES8+.StoreMetadata
- ES8+.ReplaceSessionKeys
- ES8+.LoadProfileElements.

The TSF shall permit the LPAd to transmit the following operations:

- ES10a.GetEuiccConfiguredAddresses
- ES10a.SetDefaultDpAddress
- ES10b.PrepareDownload
- ES10b.LoadBoundProfilePackage
- ES10b.GetEUICCChallenge
- ES10b.GetEUICCInfo
- ES10b.ListNotification
- ES10b.RetrieveNotificationsList
- ES10b.RemoveNotificationFromList
- ES10b.AuthenticateServer
- ES10b.CancelSession
- ES10c.GetProfilesInfo
- ES10c.EnableProfile
- ES10c.DisableProfile
- ES10c.DeleteProfile
- ES10c.eUICCMemoryReset
- ES10c.GetEID
- ES10c.SetNickname
- ES10c.GetRAT.

The TSF shall permit the remote OTA Platform to open a SCP80 or SCP81 secure channel to transmit the following operation:

- ES6.UpdateMetadata.

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

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

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

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

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

FDP_ITC.2.5/SCP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: none].

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

FPT_TDC.1.1/SCP The TSF shall provide the capability to consistently interpret
- **Commands from U.SM-DPplus and U.MNO-OTA**
- **Downloaded objects from U.SM-DPplus and U.MNO-OTA**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SCP The TSF shall use [assignment: none] when interpreting the TSF data from another trusted IT product.

FDP_UCT.1/SCP Basic data exchange confidentiality

FDP_UCT.1.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** to receive user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/SCP Data exchange integrity

FDP_UIT.1.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** to <u>receive</u> user data in a manner protected from <u>modification, deletion, insertion and replay</u> errors.

FDP_UIT.1.2/SCP The TSF shall be able to determine on receipt of user data, whether <u>modification, deletion, insertion and replay</u> has occurred.

FCS_CKM.1/SCP-SM Cryptographic key generation

FCS_CKM.1.1/SCP-SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ElGamal elliptic curves key agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following: **ECKA-EG using one of the following standards:**

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard)**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639)**
- **FRP256V1 (ANSSI ECC FRP256V1)**.

Note: in this TOE, the **FRP256V1 (ANSSI ECC FRP256V1)** is not supported

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: distribution method from SCP-SGP22 (SCP03t)] that meets the following: [assignment: SGP.02 standard].

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: wipe the buffer with random bytes] that meets the following: [assignment: none].

FCS_CKM.4/SCP-MNO Cryptographic key destruction

FCS_CKM.4.1/SCP-MNO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: invalidating memory containing the key in masked value] that meets the following: [assignment: none].

7.1.3   Security Domains

FDP_ACC.1/ISDR Subset access control

FDP_ACC.1.1/ISDR The TSF shall enforce the **ISD-R access control SFP** on

- o **subjects: S.ISD-R**
- o **objects: S.ISD-P**
- o **operations:**
    - **Create and configure profile**
    - **Store profile metadata**
    - **Enable profile**
    - **Disable profile**
    - **Delete profile**
    - **Perform a Memory reset**.

FDP_ACF.1/ISDR Security attribute based access control

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

- o **subjects: S.ISD-R**
- o **objects:**
    - **S.ISD-P with security attributes "state" and "PPR"**
- o **operations:**
    - **Create and configure profile**
    - **Store profile metadata**
    - **Enable profile**
    - **Disable profile**
    - **Delete profile**
    - **Perform a Memory reset**.

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

- o **Enabling a S.ISD-P is authorized only if**
    - **the corresponding S.ISD-P is in the state "DISABLED" and**
    - **the currently enabled S.ISD-P's PPR data allows its disabling.**
- o **Disabling a S.ISD-P is authorized only if**
    - **the corresponding S.ISD-P is in the state "ENABLED" and**
    - **the corresponding S.ISD-P's PPR data allows its disabling.**
- o **Deleting a S.ISD-P is authorized only if**
    - **the corresponding S.ISD-P is not in the state "ENABLED" and**
    - **the corresponding S.ISD-P's PPR data allows its deletion.**
- o **Performing a S.ISD-P Memory reset is authorized regardless of the involved S.ISD-P's state or PPR attribute**.

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

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

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: none].**

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

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: none].**

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

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

7.1.4 Platform Services

FDP_IFC.1/Platform_services Subset information flow control

FDP_IFC.1.1/Platform_services The TSF shall enforce the **Platform services information flow control SFP** on
users/subjects:
- o **S.ISD-R, S.ISD-P, U.MNO-SD**
- o **Platform code (S.PPE, S.PPI, S.TELECOM)**

information:
- o **D.PROFILE_NAA_PARAMS**
- o **D.PROFILE_POLICY_RULES**
- o **D.PLATFORM_RAT**

operations:
- o **installation of a profile**
- o **PPR and RAT enforcement**
- o **network authentication.**

FDP_IFF.1/Platform_services Simple security attributes

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

users/subjects:
- o **S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"**

information:
- o **D.PROFILE_NAA_PARAMS**
- o **D.PROFILE_POLICY_RULES**
- o **D.PLATFORM_RAT**

operations:
- o **installation of a profile**
- o **PPR and RAT enforcement**
- o **network authentication.**

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

- o **D.PROFILE_NAA_PARAMS shall be transmitted only:**
  - ▪ **by U.MNO-SD to S.TELECOM in order to execute the network authentication function**
  - ▪ **by S.ISD-R to S.PPI using the profile installation function**
- o **D.PROFILE_POLICY_RULES shall be transmitted only**

- ▪ **by S.ISD-R to S.PPE in order to execute the PPR enforcement function** o **D.PLATFORM_RAT shall be transmitted only**
  - ▪ **by S.ISD-R to S.PPE in order to execute the RAT enforcement function**.

FDP_IFF.1.3/Platform_services The TSF shall enforce the [assignment: none].

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

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

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:

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

7.1.5 Security management

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a [selection: hybrid physical] random number generator [selection: PTG.3] that implements: [assignment: Enhanced backward secrecy & Enhanced forward secrecy].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: [AIS31] test procedure A].

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: side channels (power consumptions and electromagnetic fluctuations)] in excess of [assignment: IC limits] enabling 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.**

FPT_EMS.1.2 The TSF shall ensure [assignment: users] are unable to use the following interface [assignment: SPCOM secure processor communication] 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.**

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1.1 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 this PP that require to be protected against unauthorized modification:
o D.MNO_KEYS
o Profile data
- D.PROFILE_NAA_PARAMS
- D.PROFILE_IDENTITY

- D.PROFILE_POLICY_RULES
- D.PROFILE_USER_CODES

o Management data

- D.PLATFORM_DATA
- D.DEVICE_INFO
- D.PLATFORM_RAT

o 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

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>deallocation of the resource from and allocation of the resource to</u> the following objects:

- o **D.SECRETS;**
- o **D.SK.EUICC.ECDSA;**
- o **The secret keys which are part of the following keysets:**
  - **D.MNO_KEYS,**
  - **D.PROFILE_NAA_PARAMS**.

FPT_FLS.1 Failure with preservation of secure state

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

- o **failure of creation of a new ISD-P by ISD-R**
- o **failure of installation of a profile by ISD-R.**

FMT_MSA.1/PLATFORM_DATA Management of security attributes

FMT_MSA.1.1/PLATFORM_DATA The TSF shall enforce the **ISD-R access control policy** to restrict the ability to <u>modify</u> the security attributes **the following parts of D.PLATFORM_DATA:**

- o **ISD-P state**

to

- o **S.ISD-R to modify ISD-P state**
  - **from "INSTALLED" to "SELECTABLE" (during ISD-P creation)**

 ▪ **from "ENABLED" to "DISABLED" (during profile disabling)**
 o **S.ISD-R to modify ISD-P state**
 ▪ **from "DISABLED" to "ENABLED" (during profile enabling)**.

FMT_MSA.1/PPR Management of security attributes

FMT_MSA.1.1/PPR The TSF shall enforce the **Security Channel protocol information flow SFP, ISD-P content access control SFP and ISD-R access control SFP** to restrict the ability to <u>change default, query, modify and delete</u> the security attributes

 o **D.PROFILE_POLICY_RULES**

 to

 o **S.ISD-R to change_default, via function "ES8.ConfigureISDP"**
 o **S.ISD-R to query**
 o **S.ISD-P to modify, via function "ES6.UpdateMetadata"**
 o **S.ISD-R to delete, via function "ES10c.DeleteProfile".**

FMT_MSA.1/CERT_KEYS Management of security attributes

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

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

to

 o **S.ISD-R for:**
 ▪ **query D.PK.CI.ECDSA**
 ▪ **delete D.MNO_KEYS, via function "ES10c.DeleteProfile"**
 o **no actor for other operations.**

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: following list of management functions].

List of management functions:

 • SCP information flow control (linked to roles S.ISD-R, U.SM-DPplus, S.ISD-P, U.MNO-SD, U.MNO-OTA)
 • Platform services information flow control (linked to roles S.PPI, S.ISD-P, S.ISD-R, U.MNO-SD)
 • ISD-R access control (linked to role S.ISD-R, U.SM-DPplus)
 • ISD-P content access control (linked to roles S.ISD-P, U.MNO-SD, U.MNO-OTA)

- ECASD access control (linked to roles S.ECASD)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- o **External users:**
  - ▪ **U.SM-DPplus**
  - ▪ **U.MNO-SD**
  - ▪ **U.MNO-OTA**
- o **Subjects:**
  - ▪ **S.ISD-R**
  - ▪ **S.ISD-P**
  - ▪ **S.ECASD**
  - ▪ **S.PPI**
  - ▪ **S.PPE**
  - ▪ **S.TELECOM**.

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

FMT_MSA.1/RAT Management of security attributes

FMT_MSA.1.1/RAT The TSF shall enforce the **Platform services information flow SFP and ISD-R access control SFP** to restrict the ability to <u>query</u> the security attributes

- o **D.PLATFORM_RAT**

to

- o **S.ISD-R to query**
- o **S.PPE to query.**

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Security Channel Protocol information flow control SFP, ISD-P content access control SFP, ISD-R access control SFP and ECASD access control SFP** to provide <u>restrictive</u> default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **no actor** to specify alternative initial values to override the default values when an object or information is created.

7.1.6   Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, Tuak, [selection: CAVE]** and cryptographic key sizes **according to the corresponding standard** that meet the following:

- o **MILENAGE according to standard [20] 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 [20]
  - Tuak according to [21] 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 TIA TR-45.AHAG Common Cryptographic Algorithms**

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: following key distribution methods] that meets the following: [assignment: following standards].

Item	Method	Standard
Milenage	distribution method from SCP-SGP22 (SCP03t)	[SGP.02]
Tuak	distribution method from SCP-SGP22 (SCP03t)	[SGP.02]
CAVE	distribution method from SCP-SGP22 (SCP03t)	[SGP.02]

FCS_CKM.4/Mobile_network Cryptographic key destruction

FCS_CKM.4.1/Mobile_network The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: invalidating memory containing the key in masked value] that meets the following: [assignment: none].

7.2 Runtime Environment Security Requirements

The Subjects (prefixed with an "S"), the Objects (prefixed with an "O"), Information (prefixed with an "I") are defined and described in [PP-JCS] section 7.1. Security attributes linked to these subjects, objects and information are also defined in [PP-JCS] section 7.1. Finally, Operations (prefixed with "OP") definition and description are present in [PP-JCS] section 7.1.

7.2.1 CoreLG Security Functional requirements

7.2.1.1 Firewall Policy

FDP_ACC.2/FIREWALL Complete access control

FDP_ACC.2.1/FIREWALL The TSF shall enforce the **FIREWALL access control SFP** on **S.PACKAGE, S.JCRE, S.JCVM, O.JAVAOBJECT** and all operations among subjects and objects covered by the SFP.

> **Refinement**:
> The operations involved in the policy are:
> - OP.CREATE,
> - OP.INVK_INTERFACE,
> - OP.INVK_VIRTUAL,
> - OP.JAVA,
> - OP.THROW,
> - OP.TYPE_ACCESS
> - OP.ARRAY_LENGTH,
> - OP.ARRAY_T_ALOAD,
> - OP.ARRAY_T_ASTORE,
> - OP.ARRAY_AASTORE.

FDP_ACC.2.2/FIREWALL The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/FIREWALL Security attribute based access control

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

Subject/Object	Security attributes
S.PACKAGE	LC Selection Status
S.JCVM	Active Applets, Currently Active Context
S.JCRE	Selected Applet Context
O.JAVAOBJECT	Sharing, Context, LifeTime

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

- ▪ **R.JAVA.1 ([JCRE3], §6.2.8): S.PACKAGE may freely perform OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or**

OP.TYPE_ACCESS upon any O.JAVAOBJECT whose Sharing attribute has value "JCRE entry point" or "global array".

- **R.JAVA.2 ([JCRE3], §6.2.8):** S.PACKAGE may freely perform OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE or OP.THROW upon any O.JAVAOBJECT whose Sharing attribute has value "Standard" and whose Lifetime attribute has value "PERSISTENT" only if O.JAVAOBJECT's Context attribute has the same value as the active context.
- **R.JAVA.3 ([JCRE3], §6.2.8.10):** S.PACKAGE may perform OP.TYPE_ACCESS upon an O.JAVAOBJECT whose Sharing attribute has value "SIO" only if O.JAVAOBJECT is being cast into (checkcast) or is being verified as being an instance of (instanceof) an interface that extends the Shareable interface.
- **R.JAVA.4 ([JCRE3], §6.2.8.6):** S.PACKAGE may perform OP.INVK_INTERFACE upon an O.JAVAOBJECT whose Sharing attribute has the value "SIO", and whose Context attribute has the value "Package AID", only if the invoked interface method extends the Shareable interface and one of the following conditions applies:
    a) The value of the attribute Selection Status of the package whose AID is "Package AID" is "Multiselectable",
    b) The value of the attribute Selection Status of the package whose AID is "Package AID" is "Non-multiselectable", and either "Package AID" is the value of the currently selected applet or otherwise "Package AID" does not occur in the attribute Active Applets.
- **R.JAVA.5:** S.PACKAGE may perform OP.CREATE only if the value of the Sharing parameter is "Standard".
- **R.JAVA.6 ([JCRE3], §6.2.8):** S.CAP_FILE may freely perform OP.ARRAY_ACCESS or OP.ARRAY_LENGTH upon any O.JAVAOBJECT whose Sharing attribute has value "global array".

FDP_ACF.1.3/FIREWALL The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

1) The subject S.JCRE can freely perform OP.JAVA(") and OP.CREATE, with the exception given in FDP_ACF.1.4/FIREWALL, provided it is the Currently Active Context.

2) The only means that the subject S.JCVM shall provide for an application to execute native code is the invocation of a Java Card API method (through OP.INVK_INTERFACE or OP.INVK_VIRTUAL).

FDP_ACF.1.4/FIREWALL The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1) Any subject with OP.JAVA upon an O.JAVAOBJECT whose LifeTime attribute has value "CLEAR_ON_DESELECT" if O.JAVAOBJECT's Context attribute is not the same as the Selected Applet Context.

2) Any subject attempting to create an object by the means of OP.CREATE and a "CLEAR_ON_DESELECT" LifeTime parameter if the active context is not the same as the Selected Applet Context.

3) S.CAP_FILE performing OP.ARRAY_AASTORE of the reference of an O.JAVAOBJECT whose sharing attribute has value "global array" or "Temporary".

4) S.CAP_FILE performing OP.PUTFIELD or OP.PUTSTATIC of the reference of an O.JAVAOBJECT whose sharing attribute has value "global array" or "Temporary".

5) **R.JAVA.7 ([JCRE3], §6.2.8.2): S.CAP_FILE performing OP.ARRAY_T_ASTORE into an array view without ATTR_WRITABLE_VIEW access attribute.**
6) **R.JAVA.8 ([JCRE3], §6.2.8.2):S.CAP_FILE performing OP.ARRAY_T_ALOAD into an array view without ATTR_READABLE_VIEW access attribute.**

FDP_IFC.1/JCVM Subset information flow control

FDP_IFC.1.1/JCVM The TSF shall enforce the **JCVM information flow control SFP** on **S.JCVM, S.LOCAL, S.MEMBER, I.DATA and OP.PUT(S1, S2, I)**.

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes
S.JCVM	Currently Active Context

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

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

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

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

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

FDP_RIP.1/OBJECTS Subset residual information protection

FDP_RIP.1.1/OBJECTS The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to** the following objects: **class instances and arrays**.

FMT_MSA.1/JCRE Management of security attributes

FMT_MSA.1.1/JCRE The TSF shall enforce the **FIREWALL access control SFP** to restrict the ability to **modify** the security attributes **Selected Applet Context** to **the Java Card RE**.

FMT_MSA.1/JCVM Management of security attributes

> **FMT_MSA.1.1/JCVM** The TSF shall enforce the **FIREWALL access control SFP and the JCVM information flow control SFP** to restrict the ability to **modify** the security attributes **Currently Active Context and Active Applets** to **the Java Card VM (S.JCVM)**.

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

> **FMT_MSA.2.1/FIREWALL_JCVM** The TSF shall ensure that only secure values are accepted for **all the security attributes of subjects and objects defined in the FIREWALL access control SFP and the JCVM information flow control SFP**.

FMT_MSA.3/FIREWALL Static attribute initialisation

> **FMT_MSA.3.1/FIREWALL** The TSF shall enforce the **FIREWALL access control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

> **FMT_MSA.3.2/FIREWALL [Editorially Refined]** The TSF shall not allow **any role** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/JCVM Static attribute initialisation

> **FMT_MSA.3.1/JCVM** The TSF shall enforce the **JCVM information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

> **FMT_MSA.3.2/JCVM [Editorially Refined]** The TSF shall not allow **any role** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/JC Specification of Management Functions

> **FMT_SMF.1.1/JC** The TSF shall be capable of performing the following management functions: **modify the Currently Active Context, the Selected Applet Context and the Active Applets**.

FMT_SMR.1/JC Security roles

> **FMT_SMR.1.1/JC** The TSF shall maintain the roles**:**
> - **JavaCard RE(JCRE),**
> - **Java Card VM (JCVM)**.

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

7.2.1.2 Application Programming Interface

FCS_CKM.1/RSA Cryptographic key generation

FCS_CKM.1.1/RSA   The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: RSA Standard and RSA CRT Key Pair Generation]** and specified cryptographic key sizes **[assignment: 512 to 2048 bits by steps of 32 bits]** that meet the following: **[assignment: see application note]**.

Application note: the keys are generated and diversified in accordance with [JCAPI3] in classes KeyBuilder (buildKey method) and KeyPair (genKeyPair method).

FCS_CKM.1/EC Cryptographic key generation

FCS_CKM.1.1/EC   The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: EC Key Pair Generation]** and specified cryptographic key sizes **[assignment: P ranging from 160 to 521 bits]** that meet the following: **[assignment: see application note]**.

Application note:
- The keys are generated and diversified in accordance with [JCAPI3] in classes KeyBuilder (buildKey method) and KeyPair (genKeyPair method).
- The TOE implements elliptic curve cryptography over GF(p), supporting the following [JCAPI3] key types:

[JCAPI3] class	Supported parameters
javacard.security.KeyBuilder	TYPE_EC_FP_PRIVATE LENGTH_EC_FP_160 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_192 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_224 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_256 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_384 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_521 TYPE_EC_FP_PRIVATE_TRANSIENT_RESET TYPE_EC_FP_PRIVATE_TRANSIENT_DESELECT
javacard.security.KeyPair	ALG_EC_FP LENGTH_EC_FP_160 ALG_EC_FP LENGTH_EC_FP_192 ALG_EC_FP LENGTH_EC_FP_224 ALG_EC_FP LENGTH_EC_FP_256 ALG_EC_FP LENGTH_EC_FP_384 ALG_EC_FP LENGTH_EC_FP_521

FCS_CKM.1/GP-SCP Cryptographic key generation

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

SCP protocol	Cryptographic algorithm	Cryptographic key size	Cryptographic standard

SCP02	TDES 2-keys	112 bits	[GPCS] section E.4.1
SCP03	AES	128, 192, 256 bits	[Amd D] section 6.2.1
SCP81	TDES 3-keys	168 bits	[Amd B] section 3.3.2
SCP81	AES	128 bits	[Amd B] section 3.3.2

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: clearKey method]** that meets the following: **[assignment: [JCAPI3] standard]**.

FCS_COP.1/TDES_MAC Cryptographic operation

FCS_COP.1.1/TDES_MAC The TSF shall perform **[assignment: MAC computation of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: MAC algorithms mentioned in the application note below]** and cryptographic key sizes **[assignment: 112 bits for TDES 2 Keys, 168 bits for TDES 3 Keys]** that meet the following: **[assignment: FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5]**.

Application note: the following TDES MACs from [JCAPI3] are implemented:

MAC length	MAC algorithm	Field name in [JCAPI3] Signature class
4 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC4_ISO9797_1_M1_ALG3
4 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC4_ISO9797_1_M2_ALG3
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_ISO9797_M1
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_ISO9797_M2
4 bytes	3DES in outer CBC mode	SIG_CIPHER_DES_MAC4
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_PKCS5
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_NOPAD
8 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC8_ISO9797_1_M1_ALG3
8 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC8_ISO9797_1_M2_ALG3
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_ISO9797_M1
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_ISO9797_M2
8 bytes	3DES in outer CBC mode	SIG_CIPHER_DES_MAC8
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_PKCS5
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_NOPAD

FCS_COP.1/AES_MAC Cryptographic operation

FCS_COP.1.1/AES_MAC The TSF shall perform **[assignment: MAC computation of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: MAC algorithms mentioned in the application note below]** and cryptographic key sizes **[assignment: 128, 192 and 256 bits]** that meet the following: **[assignment: FIPS PUB 197, NIST SP800-38A]**.

Application note: the following AES MACs from [JCAPI3] are implemented:

MAC length	MAC algorithm	Field name in [JCAPI3] Signature class
16 bytes	AES in CBC mode, block size 128 bits	ALG_AES_MAC_128_NOPAD
16 bytes	AES in CBC mode, block size 128 bits	SIG_CIPHER_AES_MAC128
16 bytes	AES in CBC mode, block size 128 bits	SIG_CIPHER_AES_CMAC128
16 bytes	AES in CBC mode, block size 128 bits	ALG_AES_CMAC_128
24 bytes	AES in CBC mode, block size 192 bits	ALG_AES_MAC_192_NOPAD
32 bytes	AES in CBC mode, block size 256 bits	ALG_AES_MAC_256_NOPAD

FCS_COP.1/ECDH Cryptographic operation

FCS_COP.1.1/ECDH The TSF shall perform **[assignment: secret key agreement]** in accordance with a specified cryptographic algorithm **[assignment: Elliptic Curve Diffie-Hellman (ECDH)]** and cryptographic key sizes **[assignment: P ranging from 160 to 521 bits]** that meet the following: **[assignment: IEEE P1363]**.

[JCAPI3] class	Implemented algorithm
KeyAgreement	ALG_EC_SVDP_DH
	ALG_EC_SVDP_DH_PLAIN

FCS_COP.1/CRC Cryptographic operation

FCS_COP.1.1/CRC The TSF shall perform **[assignment: Computation of checksum of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: CRC16 or CRC32]** and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: ISO/IEC 3309]**.

Application note: the related algorithms in [JCAPI3] are ALG_ISO3309_CRC16 and ALG_ISO3309_CRC32 (class Checksum of javacard.security).

FCS_COP.1/ECDSA_SIGN Cryptographic operation

FCS_COP.1.1/ECDSA_SIGN The TSF shall perform [**assignment: signature generation and verification**] in accordance with a specified cryptographic algorithm [**assignment: ECDSA algorithm**] and cryptographic key sizes [**assignment: NIST P-256, brainpoolP256r1**] that meet the following: [**assignment: FIPS PUB 186-4 Digital Signature Standard, RFC 5639 standard**].

[JCAPI3] class	Implemented algorithm
Signature	ALG_ECDSA_SHA
	ALG_ECDSA_SHA_224
	ALG_ECDSA_SHA_256
	ALG_ECDSA_SHA_384
	ALG_ECDSA_SHA_512
	SIG_CIPHER_ECDSA
	SIG_CIPHER_ECDSA_PLAIN

FCS_COP.1/ECKA_EG Cryptographic operation

FCS_COP.1.1/ECKA_EG The TSF shall perform **[assignment: key agreement]** in accordance with a specified cryptographic algorithm **[assignment: ECKA-EG algorithm]** and cryptographic key sizes **[assignment: NIST P-256, brainpoolP256r1]** that meet the following: [**assignment: FIPS PUB 186-3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639**].

[JCAPI3] class	Implemented algorithm
KeyAgreement	ALG_EC_SVDP_DH
	ALG_EC_SVDP_DH_PLAIN
CustomKeyAgreement	ALG_EC_SVDP_EG

FCS_COP.1/GP-SCP Cryptographic operation

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

SCP protocol	Cryptographic operation	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP02	MAC Generation/ Verification	HMAC, CMAC using TDES	112 bits	FIPS 198
SCP02	Symmetric Encryption/ Decryption	TDES in CBC mode	112 bits	NIST 800 67 NIST 800 38A
SCP02	Key Derivation	HMAC-based KDF, CMAC-based KDF using TDES	112 bits	NIST 800 108 FIPS 198
SCP03	Symmetric Encryption/ Decryption	AES in CBC mode	128, 192, or 256 bits	FIPS 197 NIST 800 38A
SCP03	MAC Generation/ Verification	CMAC AES	128, 192, or 256 bits	NIST 800 38B
SCP03	Key Derivation	CMAC-based KDF using AES	128, 192, or 256 bits	NIST 800 108 NIST 800 38B
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 112 bits AES: 128, 192, or 256 bits	TS 102 225 TS 102 226
SCP81	Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_3DES_EDE_CBC_SHA TLS_PSK_WITH_AES_128_CBC_SHA TLS_PSK_WITH_NULL_SHA TLS_PSK_WITH_AES_128_CBC_SHA256 TLS_PSK_WITH_NULL_SHA256		[Amd B] section 3.3.2
SCP-SGP22	Secure communication channel with the SM-DP+ for mutual authentication	ECKA-EG	NIST P-256, brainpoolP256r1	SGP.22 FIPS PUB 186-3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639
SCP-SGP22 (SCP03t)	Secure communication channel with the SM-DP+ for	AES	AES: 128	SGP.02

	profile download			

FCS_COP.1/TDES_CIPHER Cryptographic operation

FCS_COP.1.1/TDES_CIPHER The TSF shall perform **[assignment: encryption and decryption]** in accordance with a specified cryptographic algorithm **[assignment: TDES 2 Keys or TDES 3 Keys with cipher modes]** and cryptographic key sizes **[assignment: 112 bits for TDES 2 Keys, 168 bits for TDES 3 Keys]** that meet the following: **[assignment: FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5 standards]**.

[JCAPI3] class	Implemented algorithm	Mode
Cipher	ALG_DES_CBC_NOPAD	CBC
	ALG_DES_CBC_ISO9797_M1	CBC
	ALG_DES_CBC_ISO9797_M2	CBC
	ALG_DES_CBC_PKCS5	CBC
	ALG_DES_ECB_NOPAD	ECB
	ALG_DES_ECB_ISO9797_M1	ECB
	ALG_DES_ECB_ISO9797_M2	ECB
	ALG_DES_ECB_PKCS5	ECB

FCS_COP.1/AES_CIPHER Cryptographic operation

FCS_COP.1.1/AES_CIPHER The TSF shall perform **[assignment: encryption and decryption]** in accordance with a specified cryptographic algorithm **[assignment: AES with cipher modes]** and cryptographic key sizes **[assignment: 128, 192 and 256 bits]** that meet the following: **[assignment: FIPS PUB 197, NIST SP800-38A, NIST SP800-38D, ISO/IEC 9797-1, PKCS#5]**.

[JCAPI3] class	Implemented algorithm	Mode
Cipher	ALG_AES_BLOCK_128_CBC_NOPAD	CBC
	ALG_AES_CBC_ISO9797_M1	CBC
	ALG_AES_CBC_ISO9797_M2	CBC
	ALG_AES_CBC_PKCS5	CBC
	ALG_AES_BLOCK_128_ECB_NOPAD	ECB
	ALG_AES_ECB_ISO9797_M1	ECB
	ALG_AES_ECB_ISO9797_M2	ECB
	ALG_AES_ECB_PKCS5	ECB

FCS_COP.1/RSA_SIGN Cryptographic operation

FCS_COP.1.1/RSA_SIGN The TSF shall perform **[assignment: signature generation and signature verification]** in accordance with a specified cryptographic algorithm **[assignment: RSA Standard and RSA CRT with hash algorithms and padding schemes]** and cryptographic key sizes **[assignment: 1024 to 2048 bits (by step of 32 bits)]** that meet the following: **[assignment: PKCS#1, PKCS#1-PSS (IEEE 1363-2000), ISO/IEC 9796-2 and RFC2409]**.

[JCAPI3] class	Implemented algorithm	Padding scheme
Signature	ALG_RSA_MD5_PKCS1	PKCS#1
	ALG_RSA_MD5_PKCS1_PSS	PKCS#1-PSS scheme (IEEE 1363-2000)

	ALG_RSA_SHA_224_PKCS1	PKCS#1
	ALG_RSA_SHA_224_PKCS1_PSS	PKCS#1-PSS scheme (IEEE 1363-2000)
	ALG_RSA_SHA_256_PKCS1	PKCS#1
	ALG_RSA_SHA_256_PKCS1_PSS	PKCS#1-PSS scheme (IEEE 1363-2000)
	ALG_RSA_SHA_384_PKCS1	PKCS#1
	ALG_RSA_SHA_384_PKCS1_PSS	PKCS#1-PSS scheme (IEEE 1363-2000)
	ALG_RSA_SHA_512_PKCS1	PKCS#1
	ALG_RSA_SHA_512_PKCS1_PSS	PKCS#1-PSS scheme (IEEE 1363-2000)
	ALG_RSA_SHA_ISO9796	ISO 9796-2
	ALG_RSA_SHA_PKCS1	PKCS#1
	ALG_RSA_SHA_PKCS1_PSS	PKCS#1-PSS scheme (IEEE 1363-2000)
	SIG_CIPHER_RSA	-

FCS_COP.1/RSA_CIPHER Cryptographic operation

FCS_COP.1.1/RSA_CIPHER The TSF shall perform **[assignment: encryption and decryption]** in accordance with a specified cryptographic algorithm **[assignment: RSA Standard and RSA CRT]** and cryptographic key sizes **[assignment: 1024 to 2048 bits by steps of 32 bits]** that meet the following: **[assignment: PKCS#1, PKCS#1-OAEP scheme (IEEE 1363-2000)]**.

[JCAPI3] class	Implemented algorithm
Cipher	ALG_RSA_NOPAD
	ALG_RSA_PKCS1
	ALG_RSA_PKCS1_OAEP

FCS_COP.1/Hash Cryptographic operation

FCS_COP.1.1/Hash The TSF shall perform **[assignment: computation of a hash value]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithms]** and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: cryptographic standards]**.

[JCAPI3] class	Implemented algorithm	Standard
MessageDigest	ALG_MD5	-
	ALG_SHA	FIPS 180-4
	ALG_SHA_224	FIPS 180-4
	ALG_SHA_256	FIPS 180-4
	ALG_SHA_384	FIPS 180-4
	ALG_SHA_512	FIPS 180-4

FCS_COP.1/HMAC Cryptographic operation

FCS_COP.1.1/HMAC The TSF shall perform **[assignment: computation of a HMAC value]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithms]** and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: rfc2104]**.

[JCAPI3] class	Implemented algorithm
Signature	ALG_HMAC_MD5
	ALG_HMAC_SHA1
	ALG_HMAC_SHA_256
	ALG_HMAC_SHA_384
	ALG_HMAC_SHA_512
	SIG_CIPHER_HMAC

FDP_RIP.1/ABORT Subset residual information protection

FDP_RIP.1.1/ABORT The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **any reference to an object instance created during an aborted transaction**.

FDP_RIP.1/APDU Subset residual information protection

FDP_RIP.1.1/APDU The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to** the following objects: **the APDU buffer**.

FDP_RIP.1/bArray Subset residual information protection

FDP_RIP.1.1/bArray The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **the bArray object**.

FDP_RIP.1/GlobalArray   Subset residual information protection

FDP_RIP.1.1/GlobalArray (refined)   The TSF shall ensure that any previous information content of a resource is made unavailable upon **deallocation of the resource from** *the applet as a result of returning from the process method to* the following objects: **a user Global Array**.

Application note: An array resource is allocated when a call to the API method JCSystem.makeGlobalArray is performed. The Global Array is created as a transient JCRE Entry Point Object ensuring that reference to it cannot be retained by any application. On return from the method which called JCSystem.makeGlobalArray, the array is no longer available to any applet and is deleted and the memory in use by the array is cleared and reclaimed in the next object deletion cycle.

FDP_RIP.1/KEYS Subset residual information protection

FDP_RIP.1.1/KEYS The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **the cryptographic buffer (D.CRYPTO)**.

FDP_RIP.1/TRANSIENT Subset residual information protection

FDP_RIP.1.1/TRANSIENT The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **any transient object**.

FDP_ROL.1/FIREWALL Basic rollback

FDP_ROL.1.1/FIREWALL The TSF shall enforce **the FIREWALL access control SFP and the JCVM information flow control SFP** to permit the rollback of the **operations OP.JAVA and OP.CREATE** on the **object O.JAVAOBJECT**.

FDP_ROL.1.2/FIREWALL The TSF shall permit operations to be rolled back within the **scope of a select(), deselect(), process(), install() or uninstall() call, notwithstanding the restrictions given in [JCRE3], §7.7, within the bounds of the Commit Capacity ([JCRE3], §7.8), and those described in [JCAPI3]**.

7.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **one of the following actions:**
- o **throw an exception,**
- o **lock the card session,**
- o **reinitialize the Java Card System and its data,**
- o **[assignment: none]** upon detection of a potential security violation.

Refinement:

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

- CAP file inconsistency,
- typing error in the operands of a bytecode,
- applet life cycle inconsistency,
- card tearing (unexpected removal of the Card out of the CAD) and power failure, abort of a transaction in an unexpected context, (see abortTransaction(), [JCAPI3] and ([JCRE3], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow
- [**assignment: GlobalPlatform card state inconsistency].**

FDP_SDI.2/DATA Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **[assignment: integrity errors]** on all objects, based on the following attributes: **[assignment: integrity check data]**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **[assignment: mute the card]**.

Application note: the following data persistently stored by TOE have an integrity check data security attribute:
- Key (i.e. objects instance of classes implemented the interface Key)
- PIN (objects instance of class OwnerPin)
- Package
- GlobalPlatform card state (OP_READY, SECURED, CARD_LOCKED, TERMINATE)

The card states CARD_LOCKED and TERMINATE are not applicable to eUICC.

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **[assignment: any user]** are unable to observe the operation **[assignment: read, write, cryptographic operations]** on **[assignment: PIN, Key]** by **[assignment: any other users and/or subjects]**.

FPT_FLS.1/JC Failure with preservation of secure state

FPT_FLS.1.1/JC The TSF shall preserve a secure state when the following types of failures occur: **those associated to the potential security violations described in FAU_ARP.1**.

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use

- o **the rules defined in [JCVM3] specification,**
- o **the API tokens defined in the export files of reference implementation,**
- o **[assignment: none]** when interpreting the TSF data from another trusted IT product.

7.2.1.4 AID Management

FIA_ATD.1/AID User attribute definition

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

- o **Package AID,**
- o **Applet's version number,**
- o **Registered applet AID,**
- o **Applet Selection Status**

Refinement:
"Individual users" stand for applets.

FIA_UID.2/AID User identification before any action

FIA_UID.2.1/AID The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1/AID User-subject binding

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

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: Package AID are defined with associated value during loading and with context identifier]**.

FIA_USB.1.3/AID The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: none]**.

FMT_MTD.1/JCRE Management of TSF data

FMT_MTD.1.1/JCRE The TSF shall restrict the ability to **modify** the **list of registered applets' AIDs** to **the JCRE**.

FMT_MTD.3/JCRE Secure TSF data

FMT_MTD.3.1/JCRE The TSF shall ensure that only secure values are accepted for **the registered applets' AIDs**.

7.2.2 INSTG Security Functional requirements

This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime. The installation of applets is a critical phase, which lies partially out of the boundaries of the firewall, and therefore requires specific treatment. In this PP, loading a package or installing an applet modeled as importation of user data (that is, user application's data) with its security attributes (such as the parameters of the applet used in the firewall rules).

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

FDP_ITC.2.1/Installer The TSF shall enforce the **PACKAGE LOADING information flow control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

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

Package loading is allowed only if, for each dependent package, its AID attribute is equal to a resident package AID attribute, the major (minor) Version attribute associated to the dependent package is lesser than or equal to the major (minor) Version attribute associated to the resident package ([JCVM3], §4.5.2).

FMT_SMR.1/Installer Security roles

FMT_SMR.1.1/Installer The TSF shall maintain the roles**: Installer**.

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

FPT_FLS.1/Installer Failure with preservation of secure state

FPT_FLS.1.1/Installer The TSF shall preserve a secure state when the following types of failures occur: **the installer fails to load/install a CAP/applet as described in [JCRE3] §11.1.5**.

Application Note:
The TOE may provide additional feedback information to the card manager in case of potential security violations (see FAU_ARP.1).

FPT_RCV.3/Installer Automated recovery without undue loss

See FPT_RCV.3/GP

7.2.3   ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

FDP_ACC.2.1/ADEL The TSF shall enforce the **ADEL access control SFP** on **S.ADEL, S.JCRE, S.JCVM, O.JAVAOBJECT, O.APPLET and O.CODE_PKG** and all operations among subjects and objects covered by the SFP.

Refinement:
The operations involved in the policy are:

- OP.DELETE_APPLET,
- OP.DELETE_PCKG,
- OP.DELETE_PCKG_APPLET.

FDP_ACC.2.2/ADEL The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/ADEL Security attribute based access control

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

Subject/Object	Attributes
S.JCVM	Active Applets
S.JCRE	Selected Applet Context, Registered Applets, Resident Packages
O.CODE_PKG	Package AID, Dependent Package AID, Static References
O.APPLET	Applet Selection Status
O.JAVAOBJECT	Owner, Remote

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

In the context of this policy, an object O is reachable if and only one of the following conditions hold:
1) **the owner of O is a registered applet instance A (O is reachable from A),**
2) **a static field of a resident package P contains a reference to O (O is reachable from P),**
3) **there exists a valid remote reference to O (O is remote reachable),**
4) **there exists an object O' that is reachable according to either (1) or (2) or (3) above and O' contains a reference to O (the reachability status of O is that of O').**

The following access control rules determine when an operation among controlled subjects and objects is allowed by the policy:

- **R.JAVA.14 ([JCRE3], §11.3.4.1, Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon an O.APPLET only if,**
    1) **S.ADEL is currently selected,**
    2) **there is no instance in the context of O.APPLET that is active in any logical channel and**

> 3) **there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance distinct from O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.**
>
> o **R.JAVA.15 ([JCRE3], §11.3.4.2.1, Multiple Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon several O.APPLET only if,**
>
>> 1) **S.ADEL is currently selected,**
>> 2) **there is no instance of any of the O.APPLET being deleted that is active in any logical channel and**
>> 3) **there is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.**
>
> o **R.JAVA.16 ([JCRE3], §11.3.4.4, Applet/Library Package Deletion): S.ADEL may perform OP.DELETE_PCKG upon an O.CODE_PKG only if,**
>
>> 1) **S.ADEL is currently selected,**
>> 2) **no reachable O.JAVAOBJECT, from a package distinct from O.CODE_PKG that is an instance of a class that belongs to O.CODE_PKG, exists on the card and**
>> 3) **there is no resident package on the card that depends on O.CODE_PKG.**
>
> o **R.JAVA.17 ([JCRE3], §11.3.4.4, Applet Package and Contained Instances Deletion): S.ADEL may perform OP.DELETE_PCKG_APPLET upon an O.CODE_PKG only if,**
>
>> 1) **S.ADEL is currently selected,**
>> 2) **no reachable O.JAVAOBJECT, from a package distinct from O.CODE_PKG, which is an instance of a class that belongs to O.CODE_PKG exists on the card,**
>> 3) **there is no package loaded on the card that depends on O.CODE_PKG, and**
>> 4) **for every O.APPLET of those being deleted it holds that: (i) there is no instance in the context of O.APPLET that is active in any logical channel and (ii) there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance not being deleted, or O.JAVAOBJECT is reachable from a package not being deleted, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.**

FDP_ACF.1.3/ADEL The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/ADEL [Editorially Refined] The TSF shall explicitly deny access of **any subject but S.ADEL to O.CODE_PKG or O.APPLET for the purpose of deleting them from the card**.

FDP_RIP.1/ADEL Subset residual information protection

FDP_RIP.1.1/ADEL The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **applet instances and/or packages when one of the deletion operations in FDP_ACC.2.1/ADEL is performed on them**.

FMT_MSA.1/ADEL Management of security attributes

FMT_MSA.1.1/ADEL The TSF shall enforce the **ADEL access control SFP** to restrict the ability to **modify** the security attributes **Registered Applets and Resident Packages** to **the Java Card RE**.

FMT_MSA.3/ADEL Static attribute initialisation

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

FMT_MSA.3.2/ADEL The TSF shall allow the **following role(s): none,** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/ADEL   Specification of Management Functions

FMT_SMF.1.1/ADEL   The TSF shall be capable of performing the following management functions: **modify the list of registered applets' AIDs and the Resident CAP files**.

FMT_SMR.1/ADEL Security roles

FMT_SMR.1.1/ADEL The TSF shall maintain the roles**: applet deletion manager**.

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

FPT_FLS.1/ADEL Failure with preservation of secure state

FPT_FLS.1.1/ADEL The TSF shall preserve a secure state when the following types of failures occur: **the applet deletion manager fails to delete a CAP file/applet as described in [JCRE3], §11.3.4**.

Application Note:
The TOE may provide additional feedback information to the card manager in case of potential security violations (see FAU_ARP.1).

7.2.4   RMIG Security Functional Requirements

The product does not support RMI features.

7.2.5 ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

FDP_RIP.1.1/ODEL The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **the objects owned by the context of an applet instance which triggered the execution of the method javacard.framework.JCSystem.requestObjectDeletion()**.

FPT_FLS.1/ODEL Failure with preservation of secure state

FPT_FLS.1.1/ODEL The TSF shall preserve a secure state when the following types of failures occur: **the object deletion functions fail to delete all the unreferenced objects owned by the applet that requested the execution of the method**.

Application Note:
The TOE may provide additional feedback information to the card manager in case of potential security violations (see FAU_ARP.1).

7.2.6 CARG Security Functional Requirements

FCO_NRO.2/CM Enforced proof of origin

FCO_NRO.2.1/CM The TSF shall enforce the generation of evidence of origin for transmitted **application packages** at all times.

FCO_NRO.2.2/CM [Editorially Refined] The TSF shall be able to relate the **identity** of the originator of the information, and the **application package contained in** the information to which the evidence applies.

FCO_NRO.2.3/CM The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given **[assignment: at the time the application package is received]**.

FDP_IFC.2/CM Complete information flow control

See FDP_IFC.2/GP-ELF

FDP_IFF.1/CM Complete information flow control

See FDP_IFF.1/GP-ELF

FDP_UIT.1/CM Data exchange integrity

FDP_UIT.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to **[selection: transmit, receive]** user data in a manner protected from **[selection: modification, deletion, insertion, replay]** errors.

FDP_UIT.1.2/CM [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion, replay of some of the pieces of the application sent by the CAD** has occurred.

FIA_UID.1/CM Timing of identification

See FIA_UID.1/GP

FMT_MSA.1/CM Management of security attributes

See FMT_MSA.1/GP

FMT_MSA.3/CM Static attribute initialisation

FMT_MSA.3.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/CM The TSF shall allow the **[assignment: none]** 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: following management functions]**.

The following management functions specified in [GPCS]:
- Card and Application Security Management as defined in [GPCS]: Life Cycle, Privileges, Application/SD Locking and Unlocking, Application Status interrogation, Card Status Interrogation, command dispatch, Operational Velocity Checking.
- Management functions (Secure Channel Initiation/Operation/Termination) related to SCPs as defined in [GPCS].

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

FTP_ITC.1/CM Inter-TSF trusted channel

FTP_ITC.1.1/CM 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/CM [Editorially Refined] The TSF shall permit **the CAD placed in the card issuer secured environment** to initiate communication via the trusted channel.

FTP_ITC.1.3/CM The TSF shall initiate communication via the trusted channel for **loading/installing a new application package on the card**.

7.2.7   Global Platform Security Functional requirements

FPT_FLS.1/GP Failure with preservation of secure state

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

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

FDP_ROL.1/GP Basic rollback

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

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

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

FCO_NRO.2/GP Enforced proof of origin

FCO_NRO.2.1/GP The TSF shall enforce the generation of evidence of origin for transmitted **[assignment: Executable Load Files, SD/Application data and keys]** at all times.

Refinement:

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

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

Refinement:

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

> **FCO_NRO.2.3/GP** The TSF shall provide a capability to verify the evidence of origin of information to **the off-card entity (recipient of the evidence of origin) who requested that verification** given **[assignment: at the time the ELF, SD/Application data and keys are received]**.

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

FMT_SMR.1/GP Security roles

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

- o **On-card: S.OPEN, S.SD (e.g. ISD, APSD, CASD), Application**
- o **Off-card: Issuer, Users (e.g. VA, AP, CA) owning SDs.**

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

Application Note: this SFR refines and replaces FMT_SMR.1/Installer and FMT_SMR.1/CM of [PP-JCS], applied to roles involved in card content management operations.

FMT_SMF.1/GP Specification of Management Functions

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

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

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

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

---

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

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

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

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

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

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

o **[assignment: none].**

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

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

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

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

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

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

o **The algorithms and key sizes of the imported keys shall be supported by the SE**

o **[assignment: The Key Version Number (KVN) and the Key Identifier (Key ID) of the imported keys shall be in an allowed range as specified in section 4 of [CIC]].**

FPT_RCV.3/GP Automated recovery without undue loss

FPT_RCV.3.1/GP When automated recovery from **[assignment: none]** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/GP For **[assignment: detection of a potential loss of integrity during the transmission of an Executable Load File to the card, abortion of the installation process of an Executable Load File, or any fatal error occurred during the linking of an Executable Load File to the Executable Files already installed on the card]** the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/GP The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **[assignment: <u>0% of the Executable Load File being loaded or installed</u>]** for loss of TSF data or objects under the control of the TSF.

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

Application Note:
- This SFR refines and replaces FPT_RCV.3/Installer of [PP-JCS], applied to card content management operations
- There is no maintenance mode implemented within the TOE. Recovery is always enforced automatically as stated in FPT_RCV.3.2/GP

FDP_IFC.2/GP-ELF Complete information flow control

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

o **Subjects: S.SD, S.CAD, S.OPEN**
o **Information: APDU commands INSTALL and LOAD, GlobalPlatform APIs for loading and installing ELF** and all operations that cause that information to flow to and from subjects covered by the SFP.

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

Application Note:
- This SFR replaces FDP_IFC.2/CM of [PP-JCS].
- The subject S.SD can be the ISD, an APSD, or the CASD.
GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively

FDP_IFF.1/GP-ELF Complete information flow control

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

- o **Subjects: S.SD, S.OPEN**
- o **Information: APDU commands INSTALL and LOAD, GlobalPlatform APIs for loading and installing ELF**
- o **Security attributes: Card Life Cycle state, ELF signature verification status, ELF AID, SD privileges, Secure Channel Security Level]**.

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

- o **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, SCP03], each with a complete Secure Channel Key Set.**
- o **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- o **S.OPEN accepts an ELF only if its integrity and authenticity has been verified.**
- o **[assignment: S.OPEN accepts an ELF only if its AID is not already registered by the TSF]**.

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

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

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

- o **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- o **S.OPEN fails to verify the Card Life Cycle state**
- o **S.OPEN fails to verify the SD privileges.**
- o **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**
- o **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- o **S.SD fails to unwrap INSTALL or LOAD commands.**
- o **[assignment: The ELF AID is already registered within the card]**.

Application Note:
- This SFR refines and replaces FDP_IFF.1/CM of [PP-JCS].
- APDUs belonging to the policy ELF Loading information flow control SFP are described in the following references:
  - o For INSTALL, see [GPCS] section 11.5.
  - o For LOAD, see [GPCS] section 11.6.
- The INSTALL and LOAD commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.
- The Minimum Security Level of INSTALL and LOAD is 'AUTHENTICATED' as defined in [GPCS] section 10.6.
- For more details about the rules to be applied to each role of INSTALL command, refer to [GPCS] sections 9.3 and 3.4.

FIA_UID.1/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **[assignment: SD selection, Application selection, initializing a Secure Channel with the card, requesting data that identifies the card or off-card entities]** on behalf of the user to be performed before the user is identified.

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

Application Note:
-    This SFR refines and replaces FIA_UID.1/CM of [PP-JCS].

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP   The TSF shall detect when **1** unsuccessful authentication attempt occur related to **the authentication of the origin of a card management operation command**.

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

FIA_UAU.1/GP Timing of authentication

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

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

FDP_UIT.1/GP Basic data exchange integrity

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

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

FDP_UCT.1/GP Basic data exchange confidentiality

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

FTP_ITC.1/GP Inter-TSF trusted channel

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

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

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

- o **APDU commands sent to the card within a Secure Channel Session**
- o **When loading/installing a new ELF on the card**
- o **When transmitting and loading sensitive data to the card using STORE DATA or PUT KEY commands**
- o **When deleting ELFs, Applications, or Keys**
- o **[assignment: none].**

FPR_UNO.1/GP Unobservability

FPR_UNO.1.1/GP The TSF shall ensure that **SDs and Applications** are unable to observe the operation: **keys or data import (PUT KEY or STORE DATA), encryption, decryption, signature generation and verification, [assignment: none]** on **keys and data** by **the OPEN or any other SD or Application**.

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

FPT_TDC.1.1/GP The TSF shall provide the capability to consistently interpret **ELFs, SD/Application data and keys, data used to implement a Secure Channel, [assignment: none]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/GP The TSF shall use **the list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card, [assignment: none]** when interpreting the TSF data from another trusted IT product.

FDP_IFC.2/GP-KL Complete information flow control

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

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

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

FDP_IFF.1/GP-KL Complete information flow control

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

- o **Subjects: S.SD, S.OPEN**
- o **GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys**
- o **Security attributes: card Life Cycle State, Application and SD Life Cycle states, Secure Channel Security Level, SD and Application privileges]**.

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

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

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

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

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

- o **S.OPEN fails to verify the Card Life Cycle, Application and SD Life Cycle states.**
- o **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- o **S.SD fails to unwrap STORE DATA or PUT KEY.**
- o **S.SD fails to verify the security level applied to protect APDU commands.**
- o **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- o **[assignment: S.OPEN fails to verify that the targeted application implements a personalization interface].**

FMT_MSA.1/GP Management of security attributes

FMT_MSA.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to restrict the ability to **[selection: [assignment: perform the operations listed in table acting on]]** the security attributes **[assignment: mentioned in table]** to **[assignment: the authorized identified roles mentioned in table].**

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

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

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

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

Legend for tables above:
- ISD: Issuer Security Domain
- AM SD: Security Domain with Authorized Management privilege
- DM SD: Security Domain with Delegated Management privilege
- SD: Other Security Domain
- The card states CARD_LOCKED and TERMINATE are not applicable to eUICC.

FMT_MSA.3/GP Security attribute initialization

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

FMT_MSA.3.2/GP The TSF shall allow the **[assignment: none]** to specify alternative initial values to override the default values when an object or information is created.

7.2.8   Underlying platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide the test process before TOE Delivery with the capability to store **[selection: the Initialisation Data, Pre-personalisation Data, [assignment: none]]** in the **[assignment: SP-QFPROM]**.

Application Note: Initialisation and Pre-personalization data is prepared before TOE delivery but is loaded in Device OEM manufacturer factory. Personalization data consistency and self-test processes are performed at this manufacturing stage.

FPT_RCV.3/OS Automated recovery without undue loss

FPT_RCV.3.1/OS When automated recovery from **none,** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/OS For **[assignment: execution access to a memory zone reserved for TSF data, writing access to a memory zone reserved for TSF's code, and any segmentation fault performed by a Java Card applet]** the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/OS The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **[assignment:**

- o **0% of the contents of Java Card static fields, instance fields, and array positions that fall under the scope of an open transaction;**
- o **0% of the Java Card objects that were allocated into the scope of an open transaction;**
- o **0% of the contents of Java Card transient objects;**
- o **0% of theExecutable Load File being loaded when the failure occurred**

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

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

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

FPT_RCV.4/OS Function recovery

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

7.3 Security Functional Requirements Rationale

7.3.1 SFRs for eUICC rationale

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

7.3.2 SFRs for Runtime Environment rationale

The security functional requirements rationale for objectives O.RE* is extracted from [PP-JCS] and [PP-GP] and adapted depending on the implementation and the included SFRs and its iterations.

The next table shows the objectives related to [PP-eUICC] runtime environment and its translation according to [PP-eUICC] application notes for OE.RE* objectives. The security functional requirements rationale of O.RE* will be the same than the rationale for the objectives translated from JavaCard PP [PP-JCS] and are not repeated here. In case of O.CARD-MANAGEMENT, the Security Functional Requirements rationale is extracted from [PP-GP].

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

Table 19 - Runtime environment objectives conversion for SFR rationale.

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

7.3.3 SFRs for Underlying platform IC rationale

O.IC.PROOF_OF_IDENTITY coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for identification data storage as dealt with FAU_SAS.1.

O.IC.RECOVERY coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for recovery operations as dealt with in FPT_RCV.3/OS.

O.IC.SUPPORT coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for recovery operations as dealt with in FPT_RCV.4/OS.

7.3.4 SFRs dependency rationale

SFR	CC dependencies	Satisfied dependencies
FIA_UID.1/EXT	No Dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1

FIA_UAU.4/EXT	No Dependencies	
FIA_UID.1/MNO-SD	No Dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1	No Dependencies	
FIA_API.1	No Dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	No Dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP, FPT_TDC.1/SCP
FPT_TDC.1/SCP	No Dependencies	
FDP_UCT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/ECKA_EG, FCS_COP.1/GP-SCP, FCS_CKM.4/SCP-SM
FCS_CKM.2/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/SCP-MNO
FCS_CKM.4/SCP-SM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FCS_CKM.4/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	
FCS_RNG.1	No Dependencies	

FPT_EMS.1	No Dependencies	
FDP_SDI.1	No Dependencies	
FDP_RIP.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/PPR	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/PPR, FMT_MSA.1/CERT_KEYS, FMT_SMR.1, FMT_MSA.1/RAT
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/Mobile_network
FCS_CKM.2/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/PPR, FMT_MSA.1/CERT_KEYS, FMT_SMR.1, FMT_MSA.1/RAT
FCS_CKM.4/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP, FCS_CKM.4/Mobile_network
FDP_ACC.2/FIREWALL	(FDP_ACF.1)	FDP_ACF.1/FIREWALL
FDP_ACF.1/FIREWALL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/FIREWALL FMT_MSA.3/FIREWALL
FDP_IFC.1/JCVM	(FDP_IFF.1)	FDP_IFF.1/JCVM
FDP_IFF.1/JCVM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/JCVM FMT_MSA.3/JCVM
FDP_RIP.1/OBJECTS	No Dependencies	
FMT_MSA.1/JCRE	(FDP_ACC.1 or FDP_IFC.1) and	FDP_ACC.2/FIREWALL **See rationale** FMT_SMR.1/JC

	(FMT_SMF.1) and (FMT_SMR.1)	
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM FMT_SMF.1/CM FMT_SMR.1/JC
FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_SMR.1/JC
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_SMR.1/JC
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM FMT_SMR.1/JC
FMT_SMF.1/JC	No Dependencies	
FMT_SMR.1/JC	(FIA_UID.1)	FIA_UID.2/AID
FCS_CKM.1/RSA FCS_CKM.1/EC FCS_CKM.1/GP-SCP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/RSA_SIGN FCS_COP.1/RSA_CIPHER FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECDH FCS_COP.1/GP-SCP FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	
FCS_COP.1/TDES_MAC FCS_COP.1/AES_MAC FCS_COP.1/ECDH FCS_COP.1/CRC FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_COP.1/GP-SCP FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/RSA_SIGN FCS_COP.1/RSA_CIPHER FCS_COP.1/Hash FCS_COP.1/HMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA FCS_CKM.1/EC FCS_CKM.1/GP-SCP FCS_CKM.4 **See rationale**
FDP_RIP.1/ABORT	No Dependencies	
FDP_RIP.1/APDU	No Dependencies	
FDP_RIP.1/bArray	No Dependencies	
FDP_RIP.1/GlobalArray	No Dependencies	
FDP_RIP.1/KEYS	No Dependencies	
FDP_RIP.1/TRANSIENT	No Dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAA.1)	**See rationale**
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPR_FLS.1	No Dependencies	
FPT_TDC.1	No Dependencies	
FIA_ATD.1/AID	No Dependencies	
FIA_UID.2/AID	No Dependencies	
FIA_USB.1/AID	(FIA_ATD.1)	FIA_USB.1/AID

FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/CM FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ITC.2/Installer	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1/GP FTP_ITC.1/GP
FMT_SMR.1/Installer	(FIA_UID.1)	FIA_UID.1/GP
FPT_FLS.1/Installer	No Dependencies	
FPT_RCV.3/Installer	(AGD_OPE.1)	AGD_OPE.1
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No Dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL FMT_SMF.1/ADEL FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No Dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	**See rationale**
FPT_FLS.1/ADEL	No Dependencies	
FDP_RIP.1/ODEL	No Dependencies	
FPT_FLS.1/ODEL	No Dependencies	
FCO_NRO.2/CM	(FIA_UID.1)	FIA_UID.1/GP
FDP_IFC.2/CM	(FDP_IFF.1)	FDP_IFF.1/GP-ELF
FDP_IFF.1/CM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FDP_UIT.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FIA_UID.1/CM	No Dependencies	
FMT_MSA.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/CM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FMT_SMF.1/CM	(FIA_UID.1)	FIA_UID.1/GP
FTP_ITC.1/CM	No Dependencies	
FPT_FLS.1/GP	No Dependencies	
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMR.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/GP	No Dependencies	
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1/GP FTP_ITC.1/GP
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL FPT_TDC.1/GP FTP_ITC.1/GP

FPT_RCV.3/GP	(AGD_OPE.1)	AGD_OPE.1
FDP_IFC.2/GP-ELF	(FDP_IFF.1)	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FIA_UID.1/GP	No Dependencies	
FIA_AFL.1/GP	(FIA_UAU.1)	FIA_UAU.1/GP
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No Dependencies	
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FTP_ITC.1/GP	No Dependencies	
FPR_UNO.1/GP	No Dependencies	
FPT_TDC.1/GP	No Dependencies	
FDP_IFC.2/GP-KL	(FDP_IFF.1)	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-KL FMT_MSA.3/GP
FMT_MSA.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FAU_SAS.1	No Dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No Dependencies	

Table 20 – SFRs dependency table

Rationale for the exclusion of dependencies:

- **The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is unsupported.**

The dependency between FMT_MSA.1/JCRE and FMT_SMF.1 is not satisfied because no management functions are required for the Java Card RE.

- **The dependencies of FCS_COP.1/Hash are unsupported**

Hash operation does not require any key.

- **The dependencies of FCS_COP.1/CRC are unsupported**

CRC operations do not require any key.

- **The dependency FAU_SAA.1 of FAU_ARP.1 is unsupported**

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

- **The dependency FIA_UID.1 of FMT_SMR.1/ADEL is unsupported**

This ST does not require the identification of the "deletion manager" since it can be considered as part of the TSF.

8 TOE SUMMARY SPECIFICATION

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

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

8.1 eUICC security functions

8.1.1 GSMA.ProfileManagement

This security function implements the controls related to profiles management as defined by **[SGP.22]** and **[EUPP]**, encompassing the following operations:

- Profile downloading
- Profile elements installation
- Profile deletion
- Profile enable and disable

It also supports everything related to profile data isolation.

8.1.2 GSMA.ECASD

This security function handles the Embedded UICC Controlling Authority Security Domain (ECASD) management as defined by **[SGP.22].** The ECASD is responsible for secure storage of credentials required to support the required Security Domains on the eUICC.

ECASD installation, provisioning, eUICC authentication and credentials management are covered.

8.1.3 GSMA.ISDR

This security function handles the ISD-R management as defined by **[SGP.22]**. The ISD-R is responsible for the creation of new ISD-Ps and lifecycle management of all ISD-Ps.

ISD-R installation, provisioning, credentials and content management are covered.

8.1.4 GSMA.ISDP

This security function handles the ISD-P management as defined by **[SGP.22]**. The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile. The ISD-P is used for the Profile download and installation in collaboration with the Profile Package Interpreter for the decoding/interpretation of the received Profile Package.

ISD-R installation, provisioning, deletion, credentials and content management are covered.

8.1.5 GSMA.PPR

This security function implements Profile Policy Rules management as defined by **[SGP.22]**. The PPRs are defined by the Profile Owners and set by the SM-DP+ in the Profile Metadata. Upon downloading a profile with defined PPR, eUICC is required to follow these defined rules.

Secure management and processing of the PPRs are covered.

8.2 Runtime Environment security functions

8.2.1 GP.CardContentManagement

This security function provides the capability and a dedicated flow control for the loading, installation, extradition, registry update, selection and removal of card content and especially executable files and

application instances. Such features are offered to the Card Issuer and its business partners, allowing the Card Issuer to delegate card content management to an Application Provider according to privileges assigned to the various security domains on the card. It supports Delegated management (DM), Authorized management (AM) and it can use DAP or Mandated DAP verification and generation of Reception token. It also checks that only the card management commands specified and allowed at each state of the smart card's life cycle are accepted, and ill-formed ones are rejected with an appropriate error response

8.2.2   GP.KeyLoading

This security function provides the capability and a dedicated flow control for the loading of keys and other sensitive data using the GlobalPlatform STORE DATA and PUT KEY APDUs, or by using GlobalPlatform APIs for loading and storing data and keys.

8.2.3   GP.SecurityDomain

This security function provides security domain management, as SD creation, SD selection, SD privileges setting and SD deletion in SD hierarchy. It provides means to associate or extradite an application to a security domain in order to provide services (as secure channel) to the dedicated application without sharing the related keys stored in SD. It also provides Keyset Management in SD, with Key Set creation, Key set deletion, key importation, replacement, or deletion in Key Set. Security Domains are privileged Applications as defined in [GPCS] § 7, holding cryptographic keys to be used to support Secure Channel Protocol operations and/or to authorize card content management functions. There are different types of security domain with dedicated privileges and associated operations: ISD Security domain, Supplementary Security domains, and Controlling Authority Security domains.

8.2.4   GP.ISD

ISD Security domain as defined in [GPCS] §7.1.1, is the mandatory Security Domain, implicitly selected if the Application implicitly selectable on the same logical channel of the same card I/O interface is removed. It inherits of the Final Application privilege if the Application with that privilege is removed.

8.2.5   GP.SSD

Supplementary Security Domains are privileged Applications with dedicated privileges:
- Token Verification Privilege as described in [GPCS] §9.1.3.1
- Authorized Management Privilege as described in [GPCS] §9.1.3.2
- Delegated Management Privilege as described in [GPCS] §9.1.3.3
- Global Delete Privilege as described in [GPCS] §9.1.3.4
- Global Lock Privilege as described in [GPCS] §9.1.3.5
- Receipt Generation Privilege as described in [GPCS] §9.1.3.6
- Ciphered Load File Data Block Privilege as described in [GPCS] §9.1.3.7

Controlling Authority Security Domain is a supplementary Security Domain dedicated to the Controlling Authority with dedicated privileges. It contains Security Domains cryptographic keys needed to confidentially personalize an initial set of Secure Channel Keys of an APSD.

8.2.6   GP.SecureChannel

This security function provides a secure communication channel between a card and an off-card entity during an Application Session according to [GPCS], [Amd B], [Amd D], [Amd F], [TS 102.225] and [TS 102.226]. It provides an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.
A Secure Channel Session is divided into three sequential phases:

- Secure Channel Initiation when the on-card Application and the off-card entity have exchanged sufficient information enabling them to perform the required cryptographic functions. The Secure Channel Session initiation always includes (at least) the authentication of the off-card entity by the on-card Application; performing also the setting of the Command security level used for the session.
- Secure Channel Operation when the on-card Application and the off-card entity exchange data within the cryptographic protection of the Secure Channel Session. The Secure Channel services offered may vary from one Secure Channel Protocol to the other;
- Secure Channel Termination when either the on-card Application or the off-card entity determines that no further communication is required or allowed via an established Secure Channel Session.

The following services are provided by the Secure Channel:
- Entity authentication in which the card or the off-card entity proves its authenticity to the other entity through a cryptographic exchange, based on session key generation and a dedicated flow control; For SCP80, envelope APDU shall contain secured packet structure defined in [TS 102.225] §5 and Anti-replay mechanism is proposed optionally using a counter defined in [TS 102.225] §5.1.4;
- Integrity and authentication in which the receiving entity (the card or off-card entity) ensures that the data being received from the sending entity (respectively the off-card entity or card) actually came from an authenticated entity in the correct sequence and has not been altered;
- Confidentiality in which data being transmitted from the sending entity (the off-card entity or card) to the receiving entity (respectively the card or off-card entity) is not viewable by an unauthenticated entity.

The following Secure Channel Protocols are supported by the TOE: SCP02, SCP03, SCP80 and SCP81.

8.2.7   GP.GPRegistry

This security function provides management and access to the GlobalPlatform Registry used for:
- Store card management information;
- Store relevant application management information (e.g., AID, associated Security Domain and Privileges);
- Support card resource management data;
- Store Application Life Cycle information;
- Store card Life Cycle information;
- Track any counters associated with logs.

The content of the GlobalPlatform Registry may be accessed by administrative commands or by applet using a dedicated GlobalPlatform API.
Only secure values are accepted for the information stored in the GlobalPlatform registry (including Life Cycle states, Security Levels and Privileges).

8.2.8   JCS.APDUBuffer

The security function maintains a byte array buffer accessible from any applet context. This buffer is used to transfer incoming APDU header and data bytes as well as outgoing data according to [JCAPI3]. The APDU class API is designed to be transport protocol independent T=0, T=1, T=CL (as defined in ISO 7816-3).
Application note: ADPU buffer is a JCRE temporary entry point object where no associated reference can be stored in a variable or an array component.

8.2.9   JCS.ByteCodeExecution

This security function handles applet bytecode execution according to the rules defined in [JCVM3]. The JCVM execution may be summarized in JCVM interpreter start-up, bytecode execution and JCVM interpreter loop. The applet bytecode execution consists in:

- fetching the next bytecode to execute according to the applet's code flow control,
- decoding the next bytecode,
- executing the fetched bytecode.

The JCVM manages several types of objects, such as persistent objects, transient objects, persistent arrays (boolean, byte, short, int or reference), transient arrays (boolean, byte, short, int or reference) and static field images. For each type of object, different types of control are performed.

8.2.10 JCS.Firewall

This security function enforces a Firewall access control policy and a JCVM information flow control policy at runtime. It defines how accessing the following items: Static Class Fields, Array Objects, Class Instance Object Fields, Class Instance Object Methods, Standard Interface Methods, Shareable Interface Methods, Classes, Standard Interfaces, Shareable Interfaces, Array Object Methods.
Based on security attributes (Sharing, Context, Lifetime), it performs access control to object fields between objects and throws security exception when access is denied. Thus, it enforces applet isolation located in different packages and controls the access to global data containers shared by all applet instances.
The JCRE shall allocate and manage a context for each Java API package containing applets. The JCRE maintains for its own context a special system privilege so that it can perform operations that are denied to contexts of applets.

8.2.11 JCS.Package

This security function manages packages. A package is a structural item defined for naming, loading, storing, execution context definition. There are rules for package identification, for structure check and access rules definition. If inconsistent items are found during checks, an error message is sent.

8.2.12 JCS.CryptoAPI

This security function offers the following cryptographic services to applets through the JavaCard API:
- Generation of random numbers as defined in [JCAPI3] to be used for key values or challenges during external exchanges. The Random Number Generator (RNG) is hybrid deterministic and conformant to [AIS31] DRG.4, providing enhanced backward secrecy & enhanced forward secrecy. It passes [AIS31] test procedure A.
- Computation of checksum CRC16 and CRC32 conformant with ISO3309, as defined in [JCAPI3] Checksum class. Both ALG_ISO3309_CRC16 and ALG_ISO3309_CRC32 are supported.
- Encryption and decryption using TDES algorithm as defined in [JCAPI3] Cipher class. Both TDES 2-keys (112 bits key length) and TDES 3-keys (168 bits key length) are supported.
- Generation of 4-byte or 8-byte MAC using TDES algorithm as defined in [JCAPI3] Signature class. Both TDES 2-keys (112 bits key length) and TDES 3-keys (168 bits key length) are supported.
- Encryption and decryption using AES (128, 192 or 256 bits key) algorithm as defined in [JCAPI3] Cipher class.
- Generation of 16-byte, 24-byte or 32-byte MAC using AES algorithm (128, 192 or 256 bits key) in CBC mode as defined in [JCAPI3] Signature class.
- Data hash computation as defined in [JCAPI3] MessageDigest class.
- HMAC computation as defined in [JCAPI3] Signature class.
- Encryption and decryption using RSA with Standard or CRT modes, as defined in [JCAPI3] Cipher class. All key lengths from 1024 to 2048 bits (by steps of 32 bits) are supported.
- Generation and verification of RSA signatures in Standard or CRT modes, as defined in [JCAPI3] Signature class. All key lengths from 1024 to 2048 bits (by steps of 32 bits) are supported.

- Generation and verification of ECDSA signatures as defined in [JCAPI3] Signature class. Elliptic curve cryptography over GF(p) is considered here, with P ranging from 160 to 521 bits.
- Secret key agreement according to the ECDH algorithm, as defined in [JCAPI3] KeyAgreement class.
- Secret key agreement according to the DH algorithm (ALG_DH_PLAIN), as defined in [JCAPI3] KeyAgreement class. RSA key sizes ranging from 1024 to 2048 bits (by steps of 32 bits) are supported.

These operations are performed in a way to avoid revealing the key values. If the applet specifies an algorithm that the platform does not support, the JCRE refuses to perform the cryptographic operation and generates an exception.

8.2.13 JCS.KeyManagement

This security function enforces key management for the different associated operations: key building and generation, key importation, key exportation, key masking and key destruction using the standard API defined in [JCAPI3].

- Key generation implemented through KeyBuilder and/or KeyPair classes : RSA Standard and RSA CRT Key Pair Generation (1024 to 2048 bits by steps of 32 bits), ECDSA Key Pair Generation (P ranging from 160 to 521 bits).
- Key importation and exportation is done using method protecting confidentiality and integrity of key.
- Key masking protects the confidentiality of cryptographic keys from being read out from the memory. It ensures the service of accessing and modifying them.
- Key destruction (implemented through the method clearKey() of the Key class) disables the use of a key both logically and physically. Reuse is only possible after erase.

8.2.14 JCS.OwnerPIN

This security function provides to applets a means to perform user identification and authentication with the OwnerPin class conformant to [JCAPI3].
It offers to create a PIN and store it securely in the persistent memory. It allows access to PIN value only to perform a secure comparison between a PIN stored in the persistent memory and a data received as parameter.
A method returns a positive result if a valid Pin has been presented during current session. If the PIN is not blocked and the comparison is successful, the validated flag is set to and the try counter is set to its maximum, otherwise the authentication fails and the associated try counter is decremented. When the validated flag is set, it is assumed that the user is authenticated.
When the try counter reaches zero, the PIN is blocked and the authentication is no more possible until the PIN is unblocked.

8.2.15 JCS.EraseResidualData

This security function ensures that sensitive data are locked upon the following operations as defined in [JCRE3]:

- Deletion of package and/or applications,
- Deletion of objects.

They are erased when space needs to be reused for allocation of new objects.
This security function also ensures that the sensitive temporary buffers (transient object, bArray object, Global Array object, APDU buffer, Cryptographic buffer) are securely cleared after their usage with respect to their life-cycle and interface as defined in [JCRE3], transient object at reset or allocation and persistent object are erased at allocation for new object.

8.2.16 JCS.OutOfLifeDataUndisclosure

This security function ensures that sensitive data are locked until postponed erasure on the following operations: Deletion of persistent and transient objects according to [JCRE3].

8.2.17 JCS.RunTimeExecution

This security function provides a secure run time environment conformant to [JCRE3] and deals with:
- Instance registration or deletion,
- Application selection,
- Applet opcode execution,
- JCAPI methods execution,
- Logical channel management,
- APDU flow control, dispatch and buffer management,
- JCRE memory and context management,
- JCRE reference deletion,
- JCRE access rights,
- JCRE throw exception,
- JCRE security reaction.

8.2.18 JCS.Exception

This security function manages throwing of an instance of Exception class in the following cases:
- a SecurityException when an illegal access to an object is detected,
- a SystemException with an error code describing the error condition,
- a CryptoException in case of algorithm error or illegal use,
- any exception decided by the applet or the JCRE handled as temporary JCRE entry point object with associated JCAPI. It also offers a means to applet to handle exception and to JCRE to handle uncaught exception by applets.

8.2.19 OS.Atomicity

This security function performs write operations atomically on complex type or object in order to avoid incomplete update. Prior to be written, data is stored in an atomic back-up area. In case on writing interrupt, the only two possible values are: initial value if writing is not started or final value if writing is started. At next start-up, the atomic back-up area is check to finalize interrupted writing.

8.2.20 OS.MemoryManagement

This security function allocates memory areas and performs access control on them to avoid unauthorized access. It manages circular writing to avoid instable memory state. It enforces memory recovery in case of error detection. It offers (when required) confidentiality services for data storage: Ciphering / Deciphering of Data in RAM or in FLASH, Scrambling / Unscrambling of Data in RAM or in FLASH.

8.3 TSS Rationale

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

8.3.1 eUICC SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	This SFR is covered by GSMA.ISDR
FIA_UAU.1/EXT	This SFR is covered by GSMA.ECASD and GP.SecureChannel
FIA_USB.1/EXT	This SFR is covered by GSMA.ECASD and GP.SecurityDomain
FIA_UAU.4/EXT	This SFR is covered by GSMA.ECASD and GP.SecureChannel
FIA_UID.1/MNO-SD	This SFR is covered by GP.SecurityDomain
FIA_USB.1/MNO-SD	This SFR is covered by GP.SecurityDomain, GSMA.ISDP, GSMA.ECASD
FIA_ATD.1	This SFR is covered by GP.SecurityDomain and GSMA.ECASD
FIA_API.1.1	This SFR is covered by GSMA.ECASD
FDP_IFC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_IFF.1/SCP	This SFR is covered by GSMA.ProfileManagement
FTP_ITC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_ITC.2/SCP	This SFR is covered by GSMA.ProfileManagement
FPT_TDC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_UCT.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_UIT.1/SCP	This SFR is covered by GSMA.ProfileManagement
FCS_CKM.1/SCP-SM	This SFR is covered by GSMA.ProfileManagement and JCS.CryptoAPI for ECKA-EG
FCS_CKM.2/SCP-MNO	This SFR is covered by JCS.CryptoAPI
FCS_CKM.4/SCP-SM	This SFR is covered by JCS.KeyManagement
FCS_CKM.4/SCP-MNO	This SFR is covered by JCS.KeyManagement
FDP_ACC.1/ISDR	This SFR is covered by GSMA.ISDR
FDP_ACF.1/ISDR	This SFR is covered by GSMA.ISDR
FDP_ACC.1/ECASD	This SFR is covered by GSMA.ECASD
FDP_ACF.1/ECASD	This SFR is covered by GSMA.ECASD
FDP_IFC.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FDP_IFF.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FPT_FLS.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FCS_RNG.1	This SFR is covered by JCS.CryptoAPI providing AIS31 DRG.4 random number generation to applets.
FPT_EMS.1	This SFR is covered by JCS.CryptoAPI and JCS.KeyManagement
FDP_SDI.1	This SFR is covered by GSMA.ProfileManagement
FDP_RIP.1	This SFR is covered by GSMA.ProfileManagement
FPT_FLS.1	This SFR is covered by GSMA.ProfileManagement
FMT_MSA.1/PLATFORM_DATA	This SFR is covered by GSMA.ISDR
FMT_MSA.1/PPR	This SFR is covered by GSMA.PPR
FMT_MSA.1/CERT_KEYS	This SFR is covered by GSMA.ProfileManagement
FMT_SMF.1	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR
FMT_SMR.1	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR
FMT_MSA.1/RAT	This SFR is covered by GSMA.ISDR
FMT_MSA.3	This SFR is covered by GSMA.ISDR, GSMA.ISDP, GSMA.ECASD
FCS_COP.1/Mobile_network	This SFR is covered by JCS.CryptoAPI
FCS_CKM.2/Mobile_network	This SFR is covered by JCS.CryptoAPI
FCS_CKM.4/Mobile_network	This SFR is covered by JCS.KeyManagement

8.3.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	This SFR is covered by JCS.Firewall.
FDP_ACF.1/FIREWALL	This SFR is covered by JCS.Firewall.
FDP_IFC.1/JCVM	This SFR is covered by JCS.Firewall and JCS.APDUBuffer controlling unauthorized access or invalid storage of reference.
FDP_IFF.1/JCVM	This SFR is covered by JCS.Firewall.
FDP_RIP.1/OBJECTS	This SFR is covered by JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data).
FMT_MSA.1/JCRE	This SFR is covered by JCS.RunTimeExecution covering context switch and application selection.
FMT_MSA.1/JCVM	This SFR is covered by JCS.ByteCodeExecution requiring context switch for specific code execution and JCS.RunTimeExecution covering context switch and modification of the Currently Active Context according to given rules.
FMT_MSA.2/FIREWALL_JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_SMF.1/JC	This SFR is addressed by JCS.RunTimeExecution covering context management and instance registration.
FMT_SMR.1/JC	This SFR is addressed by JCS.RunTimeExecution covering JCVM and JCRE roles.
FCS_CKM.1/RSA	This SFR is addressed by JCS.KeyManagement covering key generation.
FCS_CKM.1/EC	This SFR is addressed by JCS.KeyManagement covering key generation.
FCS_CKM.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FCS_CKM.4	This SFR is addressed by JCS.KeyManagement covering key deletion.
FCS_COP.1/TDES_MAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/AES_MAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/ECDH	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/CRC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/ECDSA_SIGN	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/ECKA_EG	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/GP-SCP	This SFR is covered by GP.SecureChannel.

FCS_COP.1/TDES_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/AES_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/RSA_SIGN	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/RSA_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/Hash	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/HMAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FDP_RIP.1/ABORT	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/APDU	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/bArray	This SFR is addressed by JCS.OutOfLifeDataUndisclosure and JCS.EraseResidualData covering data erasure.
FDP_RIP.1/GlobalArray	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/KEYS	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/TRANSIENT	This SFR is covered by JCS.OutOfLifeDataUndisclosure managing the access control to transient object to be erased prior the erasure of the content in memory.
FDP_ROL.1/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering transaction rollback during specific operations.
FAU_ARP.1	This SFR is addressed by JCS.RunTimeExecution, JCS.Exception, JCS.Firewall, and OS.MemoryManagement covering exception handling with different specific operations.
FDP_SDI.2/DATA	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, OS.Atomicity and OS.MemoryManagement covering integrity handling with specific operations.
FPR_UNO.1	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, JCS.CryptoAPI and OS.MemoryManagement covering data handling with specific operations avoiding observation.
FPT_FLS.1/JC	This SFR is addressed by JCS.Exception, JCS.ByteCodeExecution, JCS.RunTimeExecution, and OS.Atomicity preserving a secure state when unexpected events occur during specific operations.
FPT_TDC.1	This SFR is covered by JCS.Package enforcing export check, CAP file translation and link specific operations.
FIA_ATD.1/AID	This SFR is covered by JCS.RunTimeExecution and GP.GPRegistry controlling applet registration and uninstallation.
FIA_UID.2/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing user identity (package AID) during applet selection and identify associated context provided.

FIA_USB.1/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing registration of each applet and associated package during its installation with its AID.
FMT_MTD.1/JCRE	This SFR is covered by JCS.RunTimeExecution offering services for applet registration and uninstallation managing associated access rights.
FMT_MTD.3/JCRE	This SFR is fully covered by JCS.RunTimeExecution managing presence and legacy of AID with ISO rules.
FDP_ITC.2/Installer	This SFR is covered by JCS.Package
FMT_SMR.1/Installer	This SFR is covered by JCS.Package
FPT_FLS.1/Installer	This SFR is covered by JCS.Package
FPT_RCV.3/Installer	This SFR is covered by JCS.Package and JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails.
FDP_ACC.2/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_ACF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_RIP.1/ADEL	This SFR is covered by GP.CardContentManagement and JCS.OutOfLifeDataUndisclosure by checking operations to avoid access to freed resources prior to its reuse.
FMT_MSA.1/ADEL	This SFR is covered by GP.GPRegistry, GP.CardContentManagement and JCS.RunTimeExecution responsible of checking rules concerning applet attributes, implicit and explicit selection rules prior to authorize deletion operation.
FMT_MSA.3/ADEL	This SFR is covered by JCS.RunTimeExecution and GP.CardContentManagement dealing with Security Attributes initialization, providing secure, restrictive default values for the security attributes of subject and objects involved in applet deletion.
FMT_SMF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.SecurityDomain and JCS.RunTimeExecution.
FMT_SMR.1/ADEL	This SFR is covered by GP.SecurityDomain maintaining the ISD and SDD roles responsible of applet deletion. This SFR is also covered by JCS.RunTimeExecution maintaining the JCRE role for applet uninstallation
FPT_FLS.1/ADEL	This SFR is covered by GP.GPRegistry, JCS.RunTimeExecution and OS.Atomicity preserving a secure state when unexpected events occur during package or instance deletion, managing the transaction part of the deletion operation by either rolling back, or completing it.
FDP_RIP.1/ODEL	This SFR is covered by JCS.EraseResidualData and OS.MemoryManagement ensuring that the content of deleted objects is erased upon the deletion and by JCS.OutOfLifeDataUndisclosure making unavailable for disclosure upon further reallocation of the freed space.
FPT_FLS.1/ODEL	This SFR is covered by JCS.RunTimeExecution and OS.MemoryManagement performing memory management to release no more used memory on unreferenced objects and preserves a secure state when unexpected events occur during object deletion.
FCO_NRO.2/CM	This SFR is addressed by GP.SecureChannel.

FDP_IFC.2/CM	This SFR is addressed by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_IFF.1/CM	This SFR is addressed by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_UIT.1/CM	This SFR is addressed by JCS.Package
FIA_UID.1/CM	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
FMT_MSA.1/CM	This SFR is addressed by JCS.Package
FMT_MSA.3/CM	This SFR is addressed by JCS.Package
FMT_SMF.1/CM	This SFR is addressed by JCS.Package, JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FTP_ITC.1/CM	This SFR is addressed by GP.SecureChannel.
FPT_FLS.1/GP	This SFR is addressed by JCS.Package, JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FDP_ROL.1/GP	This SFR is addressed by GP.CardContentManagement, GP.KeyLoading and OS.Atomicity.
FCO_NRO.2/GP	This SFR is covered by GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading: * mutual authentication between the external entity (Issuer or Application provider) and the selected security Domain, including creation of a session key, * by the verification of a (chained) MAC that the Issuer or Application provider attaches to each file or data block sent, * by the erase of the session key at the end of the session.
FMT_SMR.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain managing the roles: S.OPEN, issuer, application provider, verification authority and controlling authority.
FMT_SMF.1/GP	This SFR is covered by GP.SecurityDomain and GP.SecureChannel.
FDP_ITC.2/GP-ELF	This SFR is covered by JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations.
FDP_ITC.2/GP-KL	This SFR is covered by GP.KeyLoading.
FPT_RCV.3/GP	This SFR is addressed by JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails.
FDP_IFC.2/GP-ELF	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_IFF.1/GP-ELF	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
FIA_UID.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
FIA_AFL.1/GP	This SFR is covered by GP.SecureChannel.
FIA_UAU.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain (as for FIA_UID.1/GP).

FIA_UAU.4/GP	This SFR is covered by GP.SecureChannel.
FDP_UIT.1/GP	This SFR is covered by GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
FDP_UCT.1/GP	This SFR is covered by GP.SecureChannel which provides confidentiality protection for sensitive data (such as secret keys).
FTP_ITC.1/GP	This SFR is addressed by GP.SecureChannel.
FPR_UNO.1/GP	This SFR is covered by JCS.RunTimeExecution and JCS.CryptoAPI.
FPT_TDC.1/GP	This SFR is addressed by GP.CardContentManagement, GP.SecureChannel and GP.KeyLoading.
FDP_IFC.2/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FDP_IFF.1/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FMT_MSA.1/GP	This SFR is covered by GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.
FMT_MSA.3/GP	This SFR is covered by GP.SecureChannel providing setting of the default value.
FAU_SAS.1	This SFR is covered by OS.MemoryManagement
FPT_RCV.3/OS	This SFR is covered by OS.Atomicity.
FPT_RCV.4/OS	This SFR is covered by OS.MemoryManagement.

9 COMPOSITION WITH IC

9.1 Statement of compatibility – Threats part

IC Threats	Rationale
Part of [PP-84]	
T.Leak-Inherent	This threat is related to the information which is leaked from the TOE during usage of the Security IC in order to disclose sensitive data of the TOE. It is considered in the TOE evaluation.
T.Phys-Probing	This threat is related to physical probing of the TOE to disclose relevant information. It is considered in the TOE evaluation.
T.Malfunction	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. It is considered in the TOE evaluation.
T.Phys-Manipulation	This threat is related to physical manipulation of the Security IC. It is covered by the IC evaluation.
T.Leak-Forced	This threat is related to information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the composite TOE. It is covered by the IC evaluation.
T.Abuse-Func	This threat is related to the usage of functions of the TOE that are not allowed once the TOE Delivery and can impact the security of the TOE. It is considered in the TOE evaluation.
T.RND	This threat is related to the deficiency of random numbers. It is covered by the IC evaluation.
Added in the [ST/ITRE]	
T.Boot-Compromise	Boot TSF software of the TOE is protected against compromise. It is covered by the IC evaluation.
T.CONFID-TSF-CODE	Application TSF code of the TOE is protected against unauthorized disclosure. It is considered in the TOE evaluation.
T.CONFID-APPLI-DATA	Application data of the TOE is protected against unauthorized disclosure. It is considered in the TOE evaluation.
T.CONFID-TSF-DATA	Application TSF data of the TOE is protected against unauthorized disclosure. It is covered by the TOE evaluation.
T.INTEG-APPLI-CODE	Application code of the TOE is protected against unauthorized modification. It is considered in the TOE evaluation.
T.INTEG-TSF-CODE	Application TSF code of the TOE is protected against unauthorized modification. It is considered in the TOE evaluation.
T.INTEG-APPLI-DATA	Application data of the TOE is protected against unauthorized modification. It is considered in the TOE evaluation.
T.INTEG-TSF-DATA	Application TSF data of the TOE is protected against unauthorized modification. It is considered in the TOE evaluation.
T.AUTH-TSF-DATA	(part of) TSF data of the TOE is protected against unauthorized replacement from another device. It is considered in the TOE evaluation.
T.AUTH-APPLI-DATA	(part of) Application data of the TOE is protected against unauthorized replacement from another device. It is considered in the TOE evaluation.
T.RBP-TSF-DATA	(part of) TSF data of the TOE is protected against unauthorized replay from another device. It is considered in the TOE evaluation.
T.RBP-APPLI-DATA	(part of) Application data of the TOE is protected against unauthorized replay from another device. It is considered in the TOE evaluation.

9.2 Statement of compatibility – OSPs part

IC OSPs	Rationale
Part of [PP-84]	
P.Process-TOE	This policy is related to the accurate unique identification during IC Development and Production. It is covered by the IC evaluation.
P.Crypto-Service	From "Cryptographic Services" package. This policy is related to cryptographic functions supported by the hardware platform. It is covered by the IC evaluation.
Added in the [ST/ITRE]	
P.Least-Privilege	This policy is related to limit the access from a component to the other component of the SPU. It is covered by the IC evaluation.

9.3 Statement of compatibility – Assumptions part

IC Assumptions	Rationale
Part of [PP-84]	
A.Process-Sec-IC	This assumption ensures the security of the delivery and storage of the IC. It is covered by the ALC_DVS.2 activity of the TOE evaluation.
A.Resp-Appl	This assumption ensures that security relevant data of the current TOE are properly treated according to the IC security needs. It is covered by the ADV_IMP.1 activity of the TOE evaluation.
Added in the [ST/ITRE]	
-	-

9.4 Statement of compatibility – Security objectives for the environment part

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

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

IC OEs	Rationale
Part of [PP-84]	
OE.Process-Sec-IC	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. • During phases b, c: CfPOE • During phase e: SgOE
OE.Resp-Appl	This objective deals with the treatment of TOE user data by the TOE itself. It is covered by the ADV_IMP.1 activity of the TOE evaluation. • CfPOE
Added in the [ST/ITRE]	
-	-

9.5 Statement of compatibility – Security objectives part

IC Security objectives	Rationale
Part of [PP-84]	
O.Leak-Inherent	This objective is covered by TOE evaluation.
O.Phys-Probing	This objective is covered by TOE evaluation.
O.Malfunction	This objective is covered by TOE evaluation.
O.Phys-Manipulation	This objective is covered by the IC evaluation.
O.Leak-Forced	This objective is covered by the IC evaluation.
O.Abuse-Func	This objective is covered by the TOE evaluation.
O.Identification	This objective is covered by the IC evaluation.
O.RND	This objective is covered by the IC evaluation.
O.AES	From "AES" package This objective is covered by the IC evaluation.
O.TDES	From "TDES" package. This objective is covered by the IC evaluation.
O.SHA	From "Hash functions" package. This objective is covered by the IC evaluation.
Added in the [ST/ITRE]	
O.Defense-in-Depth	This objective is covered by the IC evaluation.
O.Secure-Boot	This objective is covered by the IC evaluation.
O.RSA	This objective is covered by the IC evaluation.
O.ECDSA	This objective is covered by the IC evaluation.
O.ECDH	This objective is covered by the IC evaluation.
O.KDF	This objective is covered by the IC evaluation.
O.HMAC	This objective is covered by the IC evaluation.
O.CMAC	This objective is covered by the IC evaluation.
O.OSData.Access	It is considered in the TOE evaluation.
O.OSData.Protect	It is considered in the TOE evaluation.
O.Reallocation	It is considered in the TOE evaluation.

9.6 Statement of compatibility – SFRs part

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

- **IP_SFR**: Irrelevant IC SFR not being used by the current TOE.
- **RP_SFR-SERV**: Relevant IC SFR being used by the current TOE to implement a security service with associated TSFI.
- **RP_SFR-MECH**: Relevant IC SFR being used by the current evaluation because of its security properties providing protection attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the IC.

IC SFRs	Rationale
Part of [PP-84]	
FRU_FLT.2	RP_SFR-MECH
FPT_FLS.1	RP_SFR-MECH
FMT_LIM.1	RP_SFR-MECH
FMT_LIM.2	RP_SFR-MECH
FAU_SAS.1	RP_SFR_SERV
FDP_SDC.1(1)	RP_SFR-MECH
FDP_SDI.2(1)	RP_SFR-MECH
FPT_PHP.3	RP_SFR-MECH
FDP_ITT.1	RP_SFR-MECH
FPT_ITT.1	RP_SFR-MECH
FDP_IFC.1	RP_SFR-MECH
FCS_RNG.1	RP_SFR_SERV
From "AES" package	
FCS_COP.1/AES	RP_SFR_SERV
FCS_CKM.4/AES	RP_SFR_SERV
From "TDES" package	
FCS_COP.1/TDES	RP_SFR_SERV
FCS_CKM.4/TDES	RP_SFR_SERV
From "Hash functions" package	
FCS_COP.1/SHA	RP_SFR_SERV
Added in the [ST/ITRE]	
From "Group 1: cryptographic functions"	
FCS_CKM.1/SYM	RP_SFR_SERV
FCS_CKM.1/KDF	IP_SFR
FCS_CKM.4/HMAC/CMAC	IP_SFR
FCS_COP.1/CMAC	IP_SFR
FCS_COP.1/HMAC	IP_SFR
FCS_CKM.1/ECDH	IP_SFR
FCS_CKM.1/ECDSA	IP_SFR
FCS_CKM.1/RSA	IP_SFR
FCS_CKM.4/RSA/ECDSA/ECDH	IP_SFR
FCS_COP.1/RSA_SIGN	IP_SFR
FCS_COP.1/RSA_ENC	IP_SFR
FCS_COP.1/ECDSA	IP_SFR
FCS_COP.1/ECDH	IP_SFR
From "Group 2: Secure boot"	
FDP_ITC.1	RP_SFR-MECH
FDP_SDI.2(2)	RP_SFR-MECH
From "Group 3: Access control policies for hardware component"	
FMT_CMT.1(1)	RP_SFR-MECH
FMT_CMT.1(2)	RP_SFR-MECH
FMT_CMT.1(3)	RP_SFR-MECH
FMT_CMT.1(4)	RP_SFR-MECH
FMT_CMT.1(5)	RP_SFR-MECH
FMT_CMT.1(6)	RP_SFR-MECH
From "Group 4: Access control policies for software-managed data"	
FDP_ACC.2	RP_SFR-MECH
FDP_ACF.1	RP_SFR-MECH
FMT_MSA.3	RP_SFR-MECH
FDP_RIP.1/Keys	RP_SFR-MECH
FDP_RIP.1/Transient	RP_SFR-MECH

From "Group 5: Protection of data stored outside the TOE"	
FDP_SDI.2(3)	RP_SFR-MECH
FDP_SDC.1(2)	RP_SFR-MECH
FDP_SDA.1	RP_SFR-MECH
FDP_SDR.1	RP_SFR-MECH

10 REFERENCES, GLOSSARY AND ABBREVIATIONS

10.1 External references

Reference	Title
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2017-04-001, version 3.1 revision 5, April 2017.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, CCMB-2017-04-002, version 3.1 revision 5, April 2017.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, CCMB-2017-04-003, version 3.1 revision 5, April 2017.
[CC-COMP]	Common Criteria Supporting Document, Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018.
[CIC]	Common Implementation Configuration v2.1, July 2018 - Ref: GPC_GUI_080
[EUPP]	TCA eUICC Profile Package Interoperable Format Test Specification v2.3.1, September 2020
[11]	[GPCS] Global Platform Card Specification v2.3.1 (GPC_SPE_034), March 2018 – ref [11] in [PP/0100] and amendments • [Amd A] Amendment A - Confidential Card Content Management, v1.1 - July 2019 (GPC_SPE_007) • [Amd B] Amendment B - Remote Application Management over HTTP, v1.1.3 - May 2015 (GPC_SPE_011) – ref [13] in [PP/0100] • [Amd D] Amendment D - Secure Channel Protocol 03, v1.1.1 - April 2020 (GPC_SPE_014) • [Amd H] Amendment H - Executable Load File Upgrade, v1.1 - March 2018 (GPC_SPE_120)
[12]	SCP80 ETSI TS 102 225, ETSI TS 102 226 – ref [12] in [PP/0100]
[JC]	Java Card Specification v3.0.5, May 2015
[JCAPI3]	Java Card 3 Platform - Java Card API, Classic Edition, Version 3.0.5, May 2015
[JCVM3]	Java Card 3 Platform - Virtual Machine Specification, Classic Edition, Version 3.0.5, May 2015
[JCRE3]	Java Card 3 Platform - Runtime Environment Specification, Classic Edition, Version 3.0.5, May 2015
[JCBV]	Java Card 3.1.0 Off-card Verifier and onwards
[PP-84]	Security IC Platform Protection Profile with Augmentation Packages version 1.0, February 2014, BSI-CC-PP-0084-2014
[PP-eUICC]	Embedded UICC for Consumer Devices Protection Profile version 1.0, June 2018, BSI-CC-PP-0100-2018 (SGP.25 v1.0 by GSMA)
[PP-JCS]	Java Card System – Open Configuration Protection Profile version 3.1, April 2020, BSI-CC-PP-0099-V2-2020 – ref [01] in [PP/0100]
[PP-GP]	Secure Element Protection Profile version 1.0, February 2021, GPC_SPE_174
[SGP.02]	Remote Provisioning Architecture for Embedded UICC Technical Specification – ref [03] in [PP/0100]
[SGP.06]	eUICC Security Assurance Principles, version 1.0, July 2020
[SGP.07]	eUICC Security Assurance Methodology, version 1.0, July 2020
[SGP.08]	Security Evaluation of Integrated eUICC, version 1.0, March 2021
[SGP.21]	Architecture Specification, version 2.4, August 2021
[SGP.22]	RSP Technical Specification, version 2.4, October 2021 – ref [24] in [PP/0100]
[SGP.23]	RSP Test Specification, version 1.11, October 2021
[SGP.24]	SGP.24 Compliance Process, Version 2.4.2, January 2022

Reference	Title
[ST/ITRE]	Security Target lite of SPU270 embedded in SM8550 SoC (Ref: 80-NU430-12, Revision AB)
[GUIDES/I-TRE]	List of documents applicable to the certified I-TRE: • Secure Processor Unit (SPU) – Anti-replay Island (ARI) Overview for SM8550 (Ref: 80-33265-16, Revision AB) • Qualcomm® Secure Processing Unit Enablement for SM8550 Devices – User Guide (Ref: 80-35348-150, Revision AC) • SM8550 Security Guidance for Secure Processing Unit Application Developers (Ref: 80-35348-152, Revision AB) • SM8550 Secure Boot Enablement (Ref: 80-35348-14, Revision AA) • SM8550 Secure Processor Unit SDK – API Reference (Ref: 80-PV579-21, Revision AE) • Qualcomm® Snapdragon™ Secure Processing Unit (SPU) Application Development User Guide (Ref: 80-NU430-7 Rev. AB) • SMT Assembly Guidelines (SM80-P0982-1, Revision E)
[SPU-APPDEV]	SM8550 Security Guidance for Secure Processing Unit Application Developers - User Guide (80-35348-152 Rev. AB)
[VER]	Global Platform Card Composition Model, Security Guidelines for Basic Applications (GPC_GUI_050, v2.0)

10.2 Internal references

Reference	Title
[GUIDES]	List of documents applicable to the certified iSIM v4.0: • Guidance for Secure application development on Thales iSIM Products (D1554666, revision 1.0) • Operational guidance of Thales iSIM v4.0 (D1554667, revision 1.0) • Preparative guidance of Thales iSIM v4.0 (D1554668, revision 1.0) • iSIM v4.0 -JTOP user guide (D1571435_UG, revision 1.0)

10.3 Glossary

Term	Definition
Application	Instance of an Executable Module after it has been installed and made selectable
Controlling Authority	A Controlling Authority is entity independent from the OEM represented on the iSIM and responsible for securing the keys creation and personalization of the Supplementary Security Domains.
DAP Block	Part of the Load File used for ensuring Load File Data Block verification
DAP Verification	A mechanism used by a Security Domain to verify that a Load File Data Block is authentic
Issuer Security Domain	The primary on-card entity providing support for the control, security, and communication requirements of the card administrator
Profile	Security Domains, UICC file system and secure objects (Keys, PIN codes…) formatted as defined by [EUPP]. A Profile can be downloaded from RSP Servers onto a eUICC by end user consent, as defined by [SGP.21] [SGP.22].
RSP Servers	GSMA-defined SM-DP+ and SM-DS servers. Used to distribute a Profile to the end user.
Security Domain	On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the Profile Issuer, an Application Provider or a Controlling Authority)
Supplementary Security Domain	A Security Domain other than the Issuer Security Domain dedicated to Application provider.
Verification Authority	The Verification Authority (VA), is a trusted third party represented on the (U)SIM card, acting on behalf of the OEM and responsible for the verification of application signatures (mandated DAP) during the loading process.

10.4 Abbreviations

CC	Common Criteria
HW	Hardware
iSIM	Integrated SIM
I-TRE	Integrated Tamper Resistant Element (e.g. TRE embedded within a SoC)
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile (see [SGP.22])
ISD-R	Issuer Security Domain Root (see [SGP.22])
LPAd	Local Profile Assistant on Device (see [SGP.22])
OEM	Original Equipment Manufacturer
OTA	Over-The-Air
PP	Protection Profile
REE	Rich Execution Environment (e.g. Android, iOS, Linux, Windows, etc.)
RMA	Return Merchandise Authorization (i.e. return a product under warranty for a replacement, refund, repair)
ST	Security Target
SW	Software
TOE	Target of Evaluation
VA	Verification Authority
CC	Common Criteria

END OF DOCUMENT