EPT 3352C
Security Target Lite
Version 1.0.1
17 December 2024
Eastcompeace Technology Co., Ltd.

Table of Contents

1 Security Target Introduction

1.1 Security Target reference

Name	EPT 3352C Security Target Lite
Version	V1.0.1
Reference	EPT_3352C_ST_Lite_1.0.1

1.2 TOE reference

Name	EPT 3352C
Version	V1.0
Reference	EPT_3352C_1.0

1.3 References

ID	Reference	Title	Version
[1]	[**CC-1**]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model	v3.1r5
[2]	[**CC-2**]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components	v3.1r5
[3]	[**CC-3**]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components	v3.1r5
[4]	[**PP-eUICC**]	Embedded UICC for Consumer Devices Protection Profile	v1.0
[5]	[**PP-JCS**]	Java Card System – Open Configuration Protection Profile	v3.1
[6]	[**PP-GP**]	Global Platform – Secure Element Protection Profile	v1.0
[7]	[**JCVM3**]	Java Card Platform - Classic Edition, Virtual Machine (Java Card VM) Specification.	v3.0.5
[8]	[**JCAPI3**]	Java Card Platform - Classic Edition, Application Programming Interface.	v3.0.5
[9]	[**JCRE3**]	Java Card Platform - Classic Edition, Runtime Environment (Java Card RE) Specification.	v3.0.5
[10]	[**PP-84**]	Security IC Platform Protection Profile with Augmentation Packages	v1.0
[11]	[**GPCS**]	GlobalPlatform Technology Card Specification March 2018	v2.3.1
[12]	**[PP-USIM]**	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations, ANSSI-CC-PP-2010/05.	v2.0.2
[13]	**[GPC-Gui]**	GlobalPlatform Card Composition Model Security Guidelines for Basic Applications. GPC_GUI_050.	v2.0
[14]	**[AIS31]**	Functionality classes and evaluation methodology for physical random number generators AIS31	v3.0
[15]	**[3GPP2S]**	3GPP2 S.S0053-0: Common Cryptographic Algorithms,	v2.0
[16]	**[3GPP2C]**	3GPP2 C.S0065-B: cdma2000 Application on UICC for Spread Spectrum Systems	v2.0
[17]	**[MILENAGE]**	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 11): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; • Document 1: General; • Document 2: Algorithm Specification; • Document 3: Implementers Test Data; • Document 4: Design Conformance Test Data; • Document 5: Summary and results of design and evaluation.	Rel. 11
[18]	**[TUAK]**	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0, release 12, December 2014.	v12.1.0 Rel. 12

ID	Reference	Title	Version
		• Document 1: Algorithm specification; • Document 2: Implementers' test data; • Document 3: Design conformance test data.	
[19]	**[SGP22]**	Remote SIM Provisioning (RSP) Technical Specification	V2.2.2
[20]	**[ST-IC]**	Public Security Target IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12	R 1.14

2 TOE overview

This section presents the architecture and common usages of the Target of Evaluation (TOE).

2.1 TOE description

The TOE is a eUICC and it follows an architecture as depicted below:

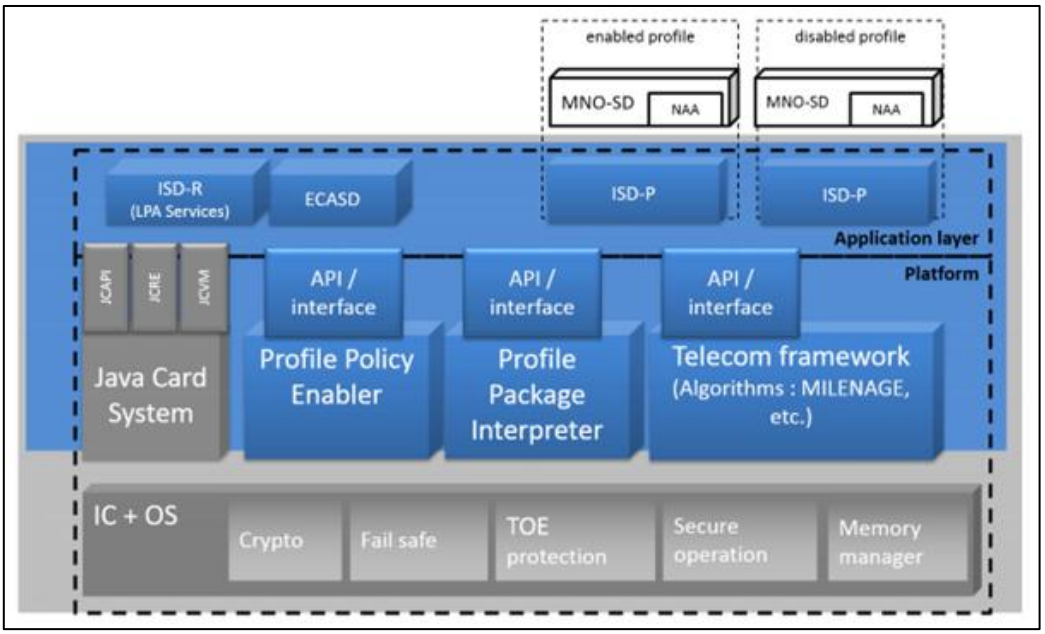

Figure 1 TOE Architecture

The TOE includes:

- The Application Layer: privileged applications, such as Security Domains, providing the remote provisioning and administration functionality (the notion of Security Domain follows the definition given by [11]):
  - An ISD-R, including LPA Services, providing life-cycle management of profiles.
  - An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication.
  - An ISD-P security domain, each one hosting a unique profile.
- The Platform Layer: a set of functions providing support to the Application Layer:
  - A Telecom Framework providing network authentication algorithms.
  - A Profile Package Interpreter translating Profile Package data into an installed Profile.
  - A Profile Policy Enabler, which comprises Profile Policy verification and enforcement, functions.
- Runtime Environment: A Java Card System built on top of an Integrated Circuit providing support to the Platform layer and Application Layer.

The Profiles are not part of the TOE.

2.2 TOE type and usage

The TOE is an UICC embedded in a consumer device, and it could be removable once it is rolled out. The eUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile.

The eUICC will contain several MNO Profiles, each of them being associated with a given International Mobile Subscriber Identity (IMSI). The primary function of the Profile is to authenticate the validity of a

Device when accessing the network. The Profile is MNO's property, and stores MNO specific information.

A eUICC with an enabled operational Profile provides the same functionality as a SIM or USIM card.

TOE major and security features are the ones described in section 1.2.1 of [4].

2.3 TOE life cycle

The TOE life cycle is based on a smartcard life cycle with differences in its post-issuance provisioning functionality.

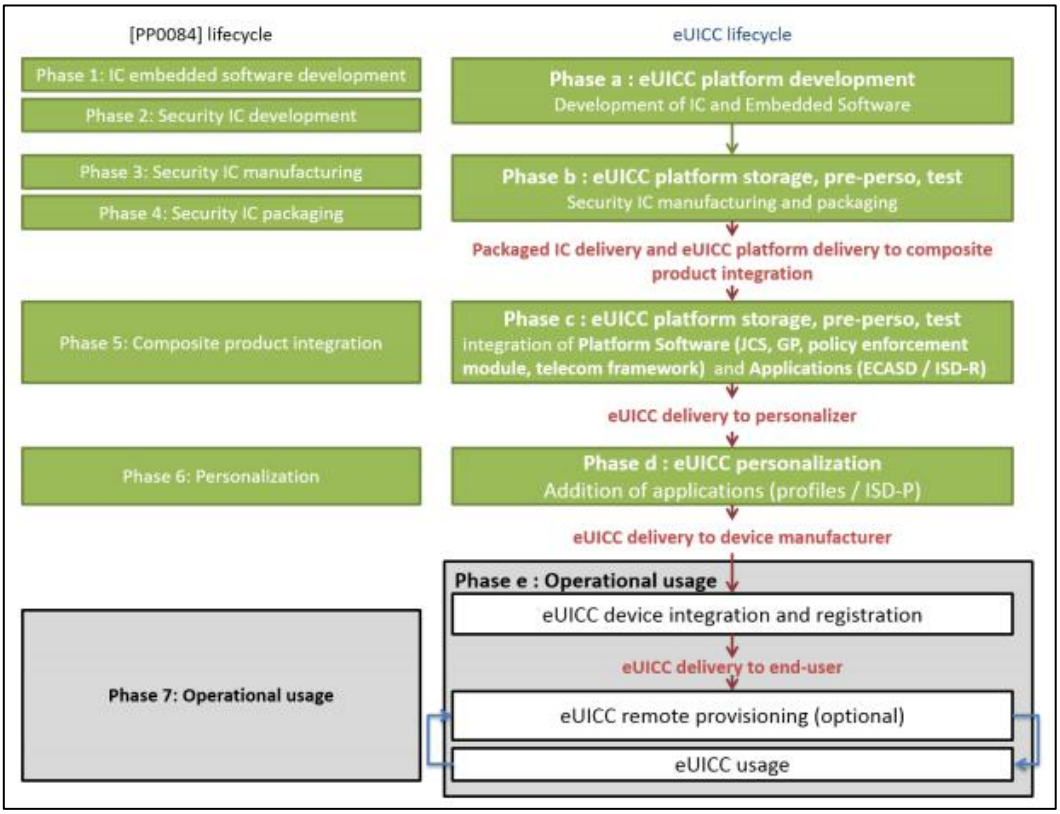

Figure 2 TOE Life Cycle

The reader may refer to [4] for a thorough description of Phases 1 to 7:

- **Phases 1 and 2** compose the product development: Embedded Software (IC Dedicated Software, OS, RE, applications, other Platform components such as PPI, PPE, and Applications) and IC development.
- **Phases 3 and 4** correspond to IC manufacturing and packaging, respectively. Some IC pre-personalization steps may occur in Phase 3.
- **Phase 5** concerns the embedding of software components within the IC.
- **Phase 6** is dedicated to the product personalization prior final use.
- **Phase 7** is the product operational phase.

The eUICC life cycle is composed of the following stages:

- **Phase a**: Development corresponds to the first two stages of the IC development.
- **Phase b**: Storage, pre-personalization and test cover the stages related to manufacturing and packaging of the IC.

- **Phase c**: eUICC platform storage, pre-personalization, test covers the stage of the embedding of software products onto the eUICC.
    - TOE Delivery: At this phase the TOE is delivered to the customer of the eUICC manufacturer.
- **Phase d**: eUICC personalization covers the insertion of provisioning Profiles and Operational Profiles onto the eUICC.
- **Phase e**: operational usage of the TOE covers the following steps:
    - eUICC integration onto the Device is performed by the Device Manufacturer. The Device Manufacturer and/or the eUICC Manufacturer also register the eUICC in a given SM-DS.
    - The eUICC is then used to provide connectivity to the Device end-user. The eUICC may be provisioned again, at post-issuance, using the remote provisioning infrastructure.

For additional details refer to section 1.2.3 of [4].

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

2.4.1 TOE interfaces

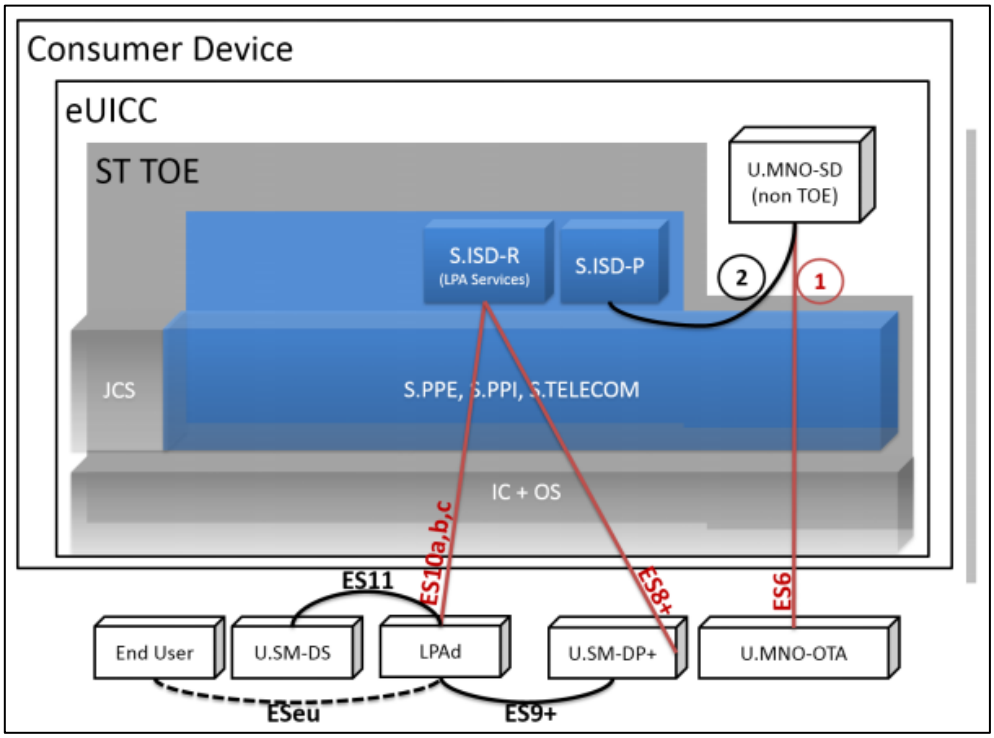

Figure 3 TOE Interfaces

As shown on Figure above, the ST TOE has the following interfaces:

- With the provisioning infrastructure, consisting in SM-DS, SM-DP+, MNO OTA Platform, and LPAd interfaces (identified ES6, ES8+, and ES10a,b,c in [19]), as well as the End User interface (ESeu).
- With the MNO-SD:
    - The interface 1 is used to enforce the trusted channel between the MNO-SD and the MNO OTA Platform.

- The interface 2 is used to enforce an internal trusted channel between the MNOSD and the ISD-P.

As the MNO-SD is not part of the TOE, a part of the enforcement of these trusted channels is ensured by the operational environment of the TOE.

All communications are supported by the Platform functions, which provide a secure APDU dispatching and support for secure communications between SDs.

The RE also supports communications by providing applications with means to protect the confidentiality and integrity of their communications (see O.RE.SECURE-COMM). The RE itself relies on the secure IC and its embedded software.

2.4.2 Description of Non-TOE HW/FW/SW and systems

- **LPAd**

  The TOE relies on a Local Profile Assistant (LPA) component. It can be either be implemented at the application level a non-TOE on-device unit called LPAd.

  Although LPAd is a non-TOE component it uses the LPA Services already mentioned in section 1.2.1.1 of [4]. In the case when LPAd is not present on the device, the interfaces ES10a, b, c are present.

- **Consumer Device**

  The eUICC is intended to be plugged in a Device from the consumer market. This equipment can be a mobile phone, or any other connecting Device featuring End User interaction.

  The consumer Device is expected to include a user interface, at least related to the eUICC functionality. For this reason, the eUICC includes the Local User Interface (LUI) part of the LPA, and it may include applications requiring user interaction such as PIN entry.

  No security certification is expected to be performed on the Device itself, and the eUICC may not rely on the Device security to protect its assets.

- **MNO-SD and applications**

  The Profile controlled by each ISD-P consists in a MNO-SD security domain, which itself may manage several applications, in the same meaning as intended by [12].

  - Basic applications: Basic applications stand for applications that do not require any particular security for their own. They must be compliant with the security rules as defined in [13].
  - Secure Applications: Secure applications are applications requiring a high level of security for their own assets. It is indeed necessary to protect application assets in confidentiality, integrity or availability at different security levels depending on the AP Security Policy. As such, secure applications follow a Common Criteria evaluation and certification in composition with the previously certified underlying Platform.

- **Remote provisioning infrastructure**

  The eUICC interfaces with the following remote provisioning entities that are responsible for the management of Profiles on the eUICC. Figure below describes the communication channels of the architecture when the LPA is located in the consumer device (LPAd).

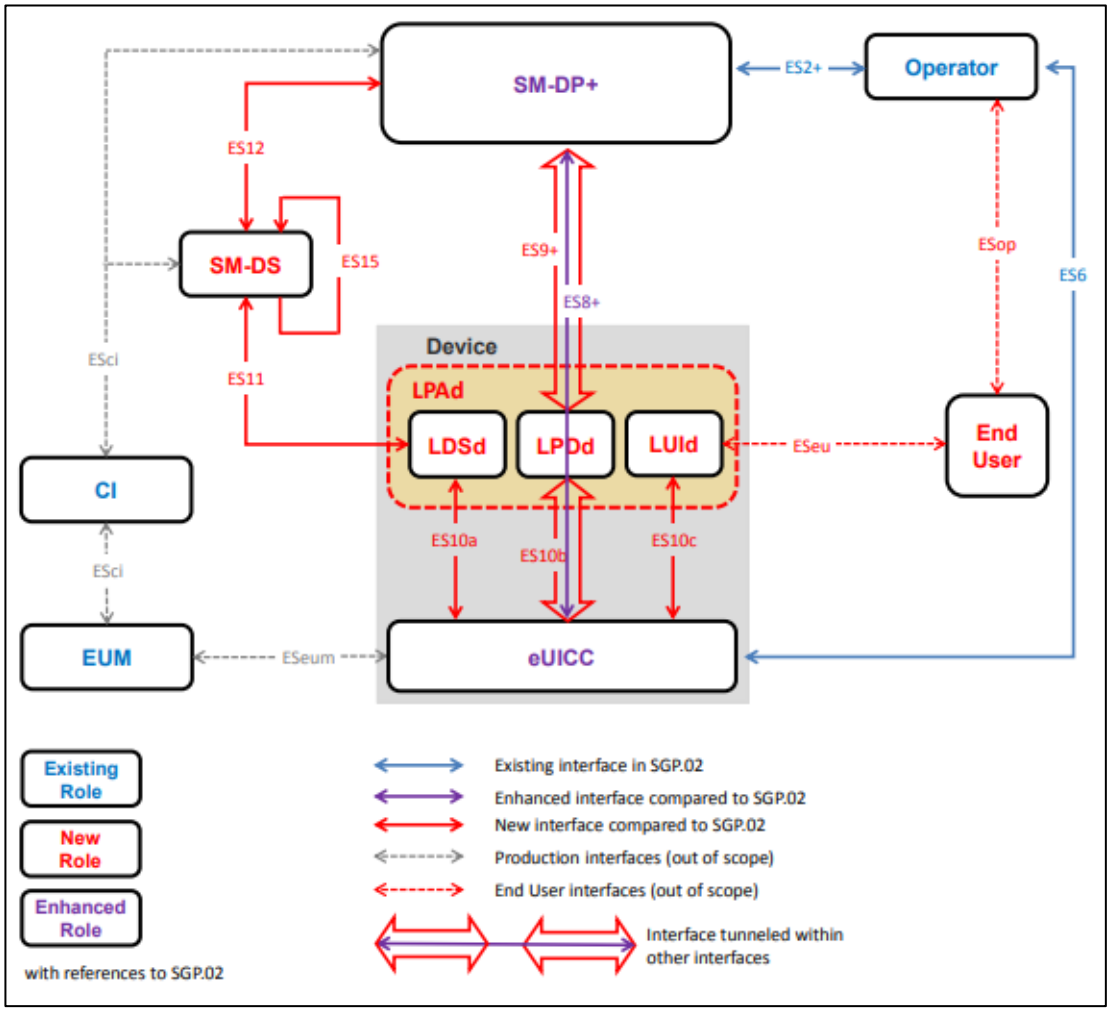

Figure 4RSP System, LPA in the Device

The TOE communicates with remote servers of:

- SM-DP+, which provides Platform and Profile management commands as well as Profiles.

The TOE shall require the use of secure channels for these interfaces. The keys and certificates required for these operations on the TOE are exchanged/generated during operational use of the TOE. Identities (in terms of certificates) rely on a single root of trust called the CI (Certificate Issuer), whose public key is stored pre-issuance on the eUICC.

The remote servers and, if any, the Devices (such a HSM) from which the keys are obtained are referred as Trusted IT products.

2.5 TOE scope

2.5.1 Physical scope

Category	Component	Version	Delivery form
HW	IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h	G12	Wafer
FW	IC Firmware	80.201.04.1	Binary file in memory
SW	ACL (EC + TOOLBOX)	v3.05.002	Binary file in memory
SW	HSL	v2.01.6198	Binary file in memory
SW	JCES	v0.1.0.9	Binary file in memory
DOC	EPT 3352C User Guidance	v1.0.8	PDF

2.5.2 Logical scope

TOE major and security features are the ones described in section 1.2.1 of [4]. Included features are as listed below:

- The Application Layer:
  - An ISD-R, including LPA Services, providing life-cycle management of profiles.
  - An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication.
  - An ISD-P security domains, each one hosting a unique profile.
- The Platform Layer
  - A Telecom Framework providing network authentication algorithms.
  - A Profile Package Interpreter translating Profile Package data into an installed Profile.
  - A Profile Policy Enabler which comprises Profile Policy verification and enforcement functions.
- Runtime Environment:
  - Java Card system; including the JCVM [7], JCAPI [8] and JCRE [9].
  - GlobalPlatform system; including Card Content Management system [11].
  - Native system; including Cryptographic primitives, Memory management and Communication protocol management.

3 Conformance Claim

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 (**BSI-DSZ-CC-1025-V6** as described in [ST-IC]), but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs 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	(R): Optional element not added in the current ST.
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 1 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 2 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.CAP_FILE		(A): Added from [PP-JCS].

Table 3 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): Additional assets (from [PP-JCS)] are mapped.
T.UNAUTHORIZED-PLATFORM-MNG	X	(R): Additional assets (from [PP-JCS)] are mapped.
T.PROFILE-MNG-INTERCEPTION	X	(R): Additional assets (from [PP-JCS)] are mapped.
T.PROFILE-MNG-ELIGIBILITY	X	(R): Additional assets (from [PP-JCS)] are mapped.
T.UNAUTHORIZED-IDENTITY-MNG	X	(R): Additional assets (from [PP-JCS)] are mapped.
T.IDENTITY-INTERCEPTION	X	(R): Additional assets (from [PP-JCS)] are mapped.
T.UNAUTHORIZED-eUICC	X	(E)
T.LPAd-INTERFACE-EXPLOIT	X	(E)
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)
T.LOGICAL-ATTACK	X	(R): Additional assets (from [PP-JCS)] are mapped.
T.PHYSICAL-ATTACK	X	(E)

Table 4 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 5 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 6 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)

Table 7 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		(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 8 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	(E)
FIA_UAU.1/EXT	X	(E)
FIA_USB.1/EXT	X	(E)
FIA_UAU.4/EXT	X	(E)
FIA_UID.1/MNO-SD	X	(E)
FIA_USB.1/MNO-SD	X	(E)

FIA_ATD.1	X	(E)
FIA_API.1	X	(E)
FDP_IFC.1/SCP	X	(E)
FDP_IFF.1/SCP	X	(E)
FTP_ITC.1/SCP	X	(E)
FDP_ITC.2/SCP	X	(E)
FPT_TDC.1/SCP	X	(E)
FDP_UCT.1/SCP	X	(E)
FDP_UIT.1/SCP	X	(E)
FCS_CKM.1/SCP-SM	X	(E)
FCS_CKM.2/SCP-MNO	X	(E)
FCS_CKM.4/SCP-SM	X	(E)
FCS_CKM.4/SCP-MNO	X	(E)
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	(E)
FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
FCS_RNG.1	X	(E)
FPT_EMS.1	X	(E)
FDP_SDI.1	X	(E)
FDP_RIP.1	X	(E)
FPT_FLS.1	X	(R): refined to definition from [PP-JCS].
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/PPR	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1	X	(E)
FMT_SMR.1	X	(E)
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.4/Mobile_network	X	(E)
FDP_ACC.2/FIREWALL		(A): Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A): Added from [PP-JCS].
FDP_IFC.1/JCVM		(A): Added from [PP-JCS].
FDP_IFF.1/JCVM		(A): Added from [PP-JCS].
FDP_RIP.1/OBJECTS		(A): Added from [PP-JCS].
FMT_MSA.1/JCRE		(A): Added from [PP-JCS].
FMT_MSA.1/JCVM		(A): Added from [PP-JCS].
FMT_MSA.2/FIREWALL_JCVM		(A): Added from [PP-JCS].

FMT_MSA.3/FIREWALL		(A): Added from [PP-JCS].
FMT_MSA.3/JCVM		(A): Added from [PP-JCS].
FMT_SMF.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FMT_SMR.1/JC		(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_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].
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/GP		(A): Added from [PP-JCS]. Iteration renamed to GP.
FMT_MSA.1/CM		(A): Added from [PP-JCS].
FMT_MSA.3/CM		(A): Added from [PP-JCS].
FMT_SMF.1/CM		(A): Added from [PP-JCS].
FMT_SMR.1/CM		(A): Added from [PP-JCS].

FTP_ITC.1/CM		(A): Added from [PP-JCS].
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].
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 [PP-GP]
FCS_COP.1/TDES	X	(A): Added to support used crypto algorithms
FCS_COP.1/AES	X	(A): Added to support used crypto algorithms
FCS_COP.1/ECKA	X	(A): Added to support used crypto algorithms
FCS_COP.1/ECDSA	X	(A): Added to support used crypto algorithms
FCS_COP.1/HASH	X	(A): Added to support used crypto algorithms
FCS_COP.1/HMAC	X	(A): Added to support used crypto algorithms

Table 9 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.

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.

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.

Refined threats description are detailed below:

- **T.UNAUTHORIZED-PROFILE-MNG**
  The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.
  Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.APP_C_DATA, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_CODE.

- **T.UNAUTHORIZED-PLATFORM-MNG**
  The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.
  Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, and D.PLATFORM_RAT. By altering the behavior of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.

- **T.PROFILE-MNG-INTERCEPTION**
  The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.
  Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.APP_C_DATA, D.PIN and D.APP_KEYs.

- **T.PROFILE-MNG-ELIGIBILITY**
  The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.
  Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, D.APP_C_DATA, D.PIN, D.APP_KEYs, D.APP_CODE and D.APP_I_DATA.

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

Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA.

- **T.IDENTITY-INTERCEPTION**
  The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.
  Directly threatens the assets: D.SECRETS, D.EID, D.APP_C_DATA, D.PIN and D.APP_KEYs.

- **T.LOGICAL-ATTACK**
  The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below.
  Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_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.

4.4 Organizational Security Policies

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

4.5 Assumptions

The definition of assumptions from [PP-eUICC] is not repeated here. See section 3.4.2.5 for complete list is assumptions.

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:

Sec. Objectives for the TOE	Description
O.IC.PROOF_OF_IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: (1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification). (2) It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.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.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 or access to an application outside of its expected availability.
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.
O.RE.API	The Runtime Environment shall ensure that native code can be invoked only via an API.
O.RE.DATA-CONFIDENTIALITY	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
O.RE.IDENTITY	The Runtime Environment shall ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.

Table 10Security Objectives for the TOE

5.2 Security Objectives for the Operational Environment

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

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 off card. The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY). 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, b, c 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] section 4.3.2.

5.3.3 Assumptions

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

A.APPLICATIONS

This assumption is directly upheld by **OE.CODE-EVIDENCE** and **OE.APPLICATIONS**

5.3.4 Rationale Tables

5.3.4.1 Threats Rationale

Threats	Sec. Objectives	Rationale
T.UNAUTHORIZEDPROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DPplus, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Sec. 5.3.1.1
T.UNAUTHORIZEDPLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Sec. 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	Sec. 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DPplus, OE.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Sec. 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	Sec. 5.3.1.2

T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Sec. 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Sec. 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	Sec. 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Sec. 5.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Sec. 5.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Sec. 5.3.1.6

Table 11 Threats and Security Objectives- Coverage

Sec. 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	N/A
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 12 Security Objectives and threats

5.3.4.2 Organizational Security Policies Rationale

OSP	Sec. Objectives	Rationale
OSP.LIFE-CYCLE	O.PPE-PPI, O.RE.PPE-PPI, O.OPERATE	Sec. 5.3.2

Table 13 Organizational Security Policies and Security Objectives- Coverage

Sec. Objectives	Organizational Security Policies
O.PPE-PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	N/A
O.SECURE-CHANNELS	N/A
O.INTERNAL-SECURE-CHANNELS	N/A
O.PROOF_OF_IDENTITY	N/A
O.OPERATE	OSP.LIFE-CYCLE
O.API	N/A
O.DATA-CONFIDENTIALITY	N/A
O.DATA-INTEGRITY	N/A
O.ALGORITHMS	N/A
OE.CI	N/A
OE.SM-DPplus	N/A
OE.MNO	N/A
O.IC.PROOF_OF_IDENTITY	N/A
O.IC.SUPPORT	N/A
O.IC.RECOVERY	N/A
O.RE.PPE-PPI	OSP.LIFE-CYCLE
O.RE.SECURE-COMM	N/A
O.RE.API	N/A
O.RE.DATA-CONFIDENTIALITY	N/A
O.RE.DATA-INTEGRITY	N/A
O.RE.IDENTITY	N/A
O.RE.CODE-EXE	N/A
OE.TRUSTED-PATHS-LPAd	N/A
OE.APPLICATIONS	N/A
OE.CODE-EVIDENCE	N/A
OE.MNO-SD	N/A
OE.SM-DS	N/A

Table 14 Security Objectives and Organizational Security Policies

5.3.4.3 Assumptions Rationale

Assumptions	Sec. Objectives for the OE	Rationale
A.TRUSTED-PATHS-LPAd	OE.TRUSTED-PATHS-LPAd	Sec. 5.3.3
A.ACTORS	OE.CI, OE.SM-DPplus, OE.MNO	Sec. 5.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	Sec. 5.3.3

Table 15 Assumptions and Security Objectives for the Operational Environment- Coverage

Sec. Objectives for the OE	Assumptions
OE.CI	A.ACTORS
OE.SM-DPplus	A.ACTORS
OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.MNO-SD	N/A

Table 16 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, and 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 Functional requirements

7.1 eUICC Security Functional Requirements

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

7.1.1 Identification and authentication

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **[assignment: initializing a secure channel with the card].**

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

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

FIA_UAU.1/EXT Timing of authentication

FIA_UAU.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **user identification**
- **[assignment: initializing a secure channel with the card]**

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

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

FIA_UAU.4/EXT Single-use authentication mechanisms

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

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow

[assignment:

- **application selection**
- **requesting data that identifies the eUICC]**

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

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

FIA_ATD.1 User attribute definition

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

FIA_API.1 Authentication Proof of Identity

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

7.1.2 Communication

FDP_IFC.1/SCP Subset information flow control

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

FDP_IFF.1/SCP Simple security attributes

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

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

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

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

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

FDP_IFF.1.4/SCP The TSF shall explicitly authorize 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:

- **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 another trusted IT product to initiate communication via the trusted channel.

Refinement:

FTP_ITC.1.3/SCP The TSF shall **permit the SM-DP+ to open a SCP-SGP22 secure channel to [assignment: 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**
- **ES10b.GetRAT**

- **ES10c.GetProfilesInfo**
- **ES10c.EnableProfile**
- **ES10c.DisableProfile**
- **ES10c.DeleteProfile**
- **ES10c.eUICCMemoryReset**
- **ES10c.GetEID**
- **ES10c.SetNickname**

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

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

FDP_UIT.1/SCP Data exchange integrity

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

FCS_CKM.1/SCP-SM Cryptographic key generation

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

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 SGP22 (SCP03t)**] that meets the following: **[assignment: SGP.22]**.

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: overwrite the keys with zeros]** 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: overwrite the keys with zeros]** that meets the following: **[assignment: none].**

7.1.3 Security Domains

FDP_ACC.1/ISDR Subset access control

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

FDP_ACF.1/ISDR Security attribute based access control

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

- **subjects: S.ISD-R**
- **objects:**
  - **S.ISD-P with security attributes "state" and "PPR"**
- **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:**

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

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

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

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

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

FDP_ACC.1/ECASD Subset access control

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

- **subjects: S.ISD-R,**
- **objects: S.ECASD,**
- **operations:**
  - **execution of a ECASD function**
  - **access to output data of these functions,**
  - **[assignment: additional operations defined by the interfaces ES8+ (SM-DP+ – eUICC), and ES10a,b,c (LPA – eUICC)**
  - **creation of a eUICC signature on material provided by an ISD-R].**

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 a eUICC signature on material provided by an ISD-R.**
  - **access to output data of these functions.**
  - **[assignment: O.SECURE-CHANNELS, O.INTERNALSECURE-CHANNELS].**

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 a eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R.**
- **[assignment: Rules defined in GSMA SGP.22 Specification].**

FDP_ACF.1.3/ECASD The TSF shall explicitly authorize 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

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

FDP_IFF.1/Platform_services Simple security attributes

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

- **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"**
- **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_POLICY_RULES**
  - **D.PLATFORM_RAT**
- **operations:**
  - **installation of a profile**
  - **PPR and RAT enforcement**
  - **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:

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

- **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 [Editorially Refined] The TSF shall enforce **[assignment: no additional information flow control SFP rules].**

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorize 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: When none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold.].**

FPT_FLS.1/Platform_services Failure with preservation of secure state

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

- **failure that lead to a potential security violation during the processing of a S.PPE, S.PPI or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **PPR and RAT enforcement**
  - **Network authentication**
- **[assignment: none].**

7.1.5 Security management

FCS_RNG.1 Random number generation

Refinement:

FCS_RNG.1.1 The TSF shall provide a **[selection: deterministic]** random number generator **[selection: Class DRG.3 according to [AIS31]** that implements: **[assignment:**

- **DRG.3.1 If initialized with a random seed using a PTRNG of class PTG.2 as random source the internal state of the RNG shall have at least 100 bit of entropy.**
- **DRG.3.2 The RNG provides forward secrecy.**
- **DRG.3.3 The RNG provides backward secrecy even if the current internal state is known.]**

FCS_RNG.1.2 The TSF shall provide **numbers in the format 8- or 16-bit** that meet **[assignment:**

- **DRG.3.4 The RNG, initialized with a random seed, where the seed has at least 100 bit of entropy and is derived by a PTG.2 certified PTRNG. The RNG generates output for which any consecutive 234 bits strings of bit length 128 are mutually different with a probability that is greater than 1 – 2^(-16).**
- **DRG.3.5 Statistical test suites cannot practically distinguish the random numbers from the output sequences of an ideal RNG. The random numbers must pass test procedure A and the U.S. National Institute of Standards and Technology (NIST) test suite for RNGs used for cryptographic purposes [S17] containing following 16 tests: Frequency (Monobit) Test, Frequency Test within a Block, Runs Tests, Test for the Longest-Run-of-Ones in a Block, Binary Matrix Rank Test, Discrete Fourier Transform (Spectral) Test, Non-overlapping (Aperiodic) Template Matching Test, Overlapping (Periodic) Template Matching Test, Maurer´s "Universal Statistical" Test, Liner Complexity Test, Serial Test, Approximate Entropy Test, Cumulative Sums (Cusums) Test, Random Excursions Test and Random Excursions Variant Test].**

Application Note:

- **The JC API is considered outside of the scope of this evaluation as a generic crypto service for third party applets.**

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **[assignment: variations in power consumption or timing during command execution]** in excess of **[assignment: non-useful information]** 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: that unauthorized users]** are unable to use the following interface **[assignment: electrical contacts or RF field]** 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

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

FDP_RIP.1 Subset residual information protection

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

FPT_FLS.1 Failure with preservation of secure state

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

FMT_MSA.1/PLATFORM_DATA Management of security attributes

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

FMT_MSA.1/PPR Management of security attributes

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

FMT_MSA.1/CERT_KEYS Management of security attributes

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

FMT_SMF.1 Specification of Management Functions

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

FMT_SMR.1 Security roles

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

FMT_MSA.1/RAT Management of security attributes

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

FCS_COP.1 Cryptographic Operation

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

Application Note:

- **The cryptographic operations are defined to support specifically the dependencies as required by Application note 25, Application note 32, Application note 35 and Application note 36 from [PP-eUICC]. The JC API is considered outside of the scope of this evaluation as a generic crypto service for third party applets.**

Iteration	Cryptographic Operation	Cryptographic Algorithm	Supported Key Size	Standards
TDES	encryption and decryption	DES – TDES with Modes CBC, ECB, and CMAC	112 or 168 bits	FIPS PUB 46-3, ANSI X3.92, FIPS PUB 81, ISO/IEC 9797(1999),
AES	encryption and decryption	AES with Modes CBC, ECB, and CMAC	128 to 256 bits with a step of 64 bits	FIPS PUB 197, SP800-38B (CMAC)
ECKA	Key agreement	ElGamal	160, 192, 256, 384, 512 and 521bits	NIST 800-56A Rev.3
ECDSA	Signature and Signature's verification	ECDSA	160, 192, 256, 384, 512 and 521bits	ANSI X9.62-1998
HASH	Hash functions	SHA-256	NA	Secure Hash Standard, FIPS PUB 180-4, FIPS 202
HMAC	Signature	HMAC	64 - 1016 bits Based on SHA-256	FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)

FMT_MSA.3 Static attribute initialization

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

7.1.6 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, Tuak, [selection: none]** and cryptographic key sizes **according to the corresponding standard** that meet the following:

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

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: distribution method from SGP22 (SCP03t)]** that meets the following: **[assignment: SGP.22].**

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: overwrite the keys with zeros]** 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

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

FDP_ACF.1/FIREWALL Security attribute based access control

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

FDP_IFC.1/JCVM Subset information flow control

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

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes
S.JCVM	Currently Active Context

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

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

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

FDP_IFF.1.4/JCVM The TSF shall explicitly authorize 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

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

FMT_MSA.1/JCRE Management of security attributes

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

FMT_MSA.1/JCVM Management of security attributes

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

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

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

FMT_MSA.3/FIREWALL Static attribute initialization

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

FMT_MSA.3/JCVM Static attribute initialization

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

FMT_SMF.1/JC Specification of Management Functions

The definition of this SFR is present in [PP-JCS] defined as FMT_SMF.1. Its formulation is unchanged within this ST.

FMT_SMR.1/JC Security roles

The definition of this SFR is present in [PP-JCS] defined as FMT_SMR.1. Its formulation is unchanged within this ST.

7.2.1.2 Application Programming Interface

FDP_RIP.1/ABORT Subset residual information protection

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

FDP_RIP.1/APDU Subset residual information protection

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

FDP_RIP.1/bArray Subset residual information protection

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

FDP_RIP.1/GlobalArray Subset residual information protection

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

FDP_RIP.1/KEYS Subset residual information protection

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

FDP_RIP.1/TRANSIENT Subset residual information protection

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

FDP_ROL.1/FIREWALL Basic rollback

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

7.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

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

- **throw an exception,**
- **lock the card session,**
- **reinitialize the Java Card System and its data,**
- **[assignment: 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: none].**

FDP_SDI.2/DATA Stored data integrity monitoring and action

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

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

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that [assignment: all users] are unable to observe the operation **[assignment: all operations]** on **[assignment: D.APP_KEYs, D.PIN]** by **[assignment: another user].**

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

- **the rules defined in [JCVM3] specification,**
- **the API tokens defined in the export files of reference implementation,**
- **[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

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

FIA_UID.2/AID User identification before any action

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

FIA_USB.1/AID User-subject binding

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

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: Each uploaded package is associated with a unique Package AID].**

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: The initially assigned Package AID is unchangeable].**

FMT_MTD.1/JCRE Management of TSF data

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

FMT_MTD.3/JCRE Secure TSF data

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

7.2.2 INSTG Security Functional requirements

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

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

FMT_SMR.1/Installer Security roles

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

FPT_FLS.1/Installer Failure with preservation of secure state

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

FPT_RCV.3/Installer Automated recovery without undue loss

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

FPT_RCV.3.3/Installer The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **[assignment: 0%]** for loss of TSF data or objects under the control of the TSF.

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

7.2.3 ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

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

FDP_ACF.1/ADEL Security attribute based access control

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

FDP_RIP.1/ADEL Subset residual information protection

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

FMT_MSA.1/ADEL Management of security attributes

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

FMT_MSA.3/ADEL Static attribute initialization

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

FMT_SMF.1/ADEL Specification of Management Functions

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

FMT_SMR.1/ADEL Security roles

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

FPT_FLS.1/ADEL Failure with preservation of secure state

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

7.2.4 RMIG Security Functional Requirements

The TOE does not support RMI features.

7.2.5 ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

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

FPT_FLS.1/ODEL Failure with preservation of secure state

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

7.2.6 CARG Security Functional Requirements

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.

Refinement:

FCO_NRO.2.3/CM The TSF shall provide a capability to verify the evidence of origin of information to **originator** given **[assignment: at the time the Executable load files are received** as no **evidence is kept on the card for future verification**].

FDP_IFC.2/CM Complete information flow control

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

FDP_IFF.1/CM Simple security attributes

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

- **Subjects:**
  - **S.CAD receiving the Card Content Management commands (through APDUs or APIs).**
- **Information:**
  - **executable load file, in case of application loading;**
  - **applications or SD privileges, in case of application installation or registry update;**
  - **personalization keys and/or certificates, in case of application or SD personalization.]**

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

- **Runtime behavior rules defined by GlobalPlatform for:**
  - **loading (Section 9.3.5 of [GPCS]);**
  - **installation (Section 9.3.6 of [GPCS**
  - **extradition (Section 9.4.1 of [GPCS]);**
  - **registry update (Section 9.4.2 of [GPCS]);**
  - **content removal (Section 9.5 of [GPCS])].**

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

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

FDP_IFF.1.5/CM The TSF shall explicitly deny an information flow based on the following rules: **The TOE fails to verify the integrity and authenticity evidences of the application package [assignment:**

- **When none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold].**

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: receive]** user data in a manner protected from **[selection: modification, deletion and 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/GP Timing of identification

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

- **application selection**
- **initializing a secure channel with the card**
- **requesting data that identifies the card or the Card Issuer]**

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.

FMT_MSA.1/CM Management of security attributes

FMT_MSA.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to restrict the ability to **[selection: modify]** the security attributes **[assignment:**

- **Key Set,**
- **Security Level,**
- **Secure Channel Protocol, • Session Keys,**
- **Sequence Counter,**
- **ICV.] to [assignment:**

the actor associated with the according security domain:

- **The Card Issuer for ISD,**
- **The Application Provider for APSD].**

FMT_MSA.3/CM Static attribute initialization

FMT_MSA.3.1/CM The TSF shall enforce the CAP FILE 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:**

Management functions specified in GlobalPlatform specifications:

- **card locking (Section 9.6.3 of [GPC])**
- **application locking and unlocking (Section 9.6.2 of [GPC])**
- **card termination (Section 9.6.4 of [GPC])**
- **card status interrogation (Section 9.6.6 of [GPC])**
- **application status interrogation (Section 9.6.5 of [GPC])]**

FMT_SMR.1/CM Security roles

FMT_SMR.1.1/CM The TSF shall maintain the roles **[assignment: Installer].**

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

FTP_ITC.1/CM Inter-TSF trusted channel

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

7.2.7 Card Content Management Security Functional requirements

FIA_UAU.1/GP Timing of authentication

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

FDP_UIT.1/GP Basic data exchange integrity

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

7.2.8 Underlying platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **[assignment: the test process before TOE Delivery]** with the capability to store **[assignment: the Initialization Data, Pre-personalization Data, Smartcard Embedded Software]** in the **[assignment: SOLID FLASHTM NVM].**

FPT_RCV.3/OS Automated recovery without undue loss

FPT_RCV.3.1/OS 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/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:

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

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 **[assignment: 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 Assurance Requirements Rationale

7.3.1 SAR – Evaluation Assurance Level Rationale

The security assurance requirements rationale is the same than the ones present in section 6.2 from [PP-eUICC].

7.3.2 SAR – Dependency rationale

SAR	CC dependencies	Satisfied dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4 ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3 ALC_TAT.1
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4 ALC_DVS.2 ALC_LCD.1
ALC_CMS.4	No dependencies	
ALC_DEL.1	No dependencies	
ALC_DVS.2	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4 ASE_INT.1 ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4

SAR	CC dependencies	Satisfied dependencies
		ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1

Table 17SAR dependency mapping

The table here-above shows that all SAR dependencies are met

7.4 Security Functional Requirements Rationale

7.4.1 SFRs for eUICC rationale

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

7.4.2 SFRs for Runtime Environment rationale

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

RE objectives	Translation from [PP-JCS] and [PP-GP]
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.NATIVE

Table 18 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.

7.4.3 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 and FPT_RCV.4/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.

7.4.4 SFR 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	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.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_CKM.4/SCP-SM FCS_COP.1/ECKA FCS_COP.1/GP-SCP
FCS_COP.1/TDES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_COP.1/AES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_COP.1/ECKA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_COP.1/ECDSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_COP.1/HASH	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_COP.1/HMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/SCP-MNO
FCS_CKM.4/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP FCS_CKM.1/SCP-SM
FCS_CKM.4/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	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	

SFR	CC dependencies	Satisfied 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 FDP_IFC.1/SCP 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 FDP_IFC.1/SCP FDP_ACC.1/ECASD 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_SMF.1	No dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT FIA_UID.1/MNO-SD
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	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/Mobile_network
FCS_CKM.4/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP
FDP_IFC.2/CM	(FDP_IFF.1)	FDP_IFF.1/CM
FDP_IFF.1/CM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/CM FMT_MSA.3/CM
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/CM FPT_TDC.1 FTP_ITC.1/CM
FMT_MSA.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/CM FMT_SMR.1/CM FMT_SMF.1/CM
FMT_MSA.3/CM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/CM FMT_SMR.1/CM
FMT_SMR.1/CM	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/CM	No dependencies	
FPT_RCV.3/Installer	(AGD_OPE.1)	AGD_OPE.1
FMT_SMR.1/Installer	(FIA_UID.1)	FIA_UID.1/GP
FPT_FLS.1/Installer	No dependencies	
FPT_TDC.1	No dependencies	
FTP_ITC.1/CM	No dependencies	
FCO_NRO.2/CM	(FIA_UID.1)	FIA_UID.1/GP
FIA_UID.1/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/CM FTP_ITC.1/CM
FDP_UIT.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM FTP_ITC.1/CM
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/CM FTP_ITC.1/CM
FPR_UNO.1	No dependencies	
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No dependencies	
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ECASD FMT_SMR.1/CM FMT_SMF.1/CM
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 (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FMT_SMR.1/JC **See rationale**
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/JC 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

SFR	CC dependencies	Satisfied dependencies
		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
FDP_RIP.1/ABORT	No dependencies	
FDP_RIP.1/APDU	No dependencies	
FDP_RIP.1/GlobalArray	No dependencies	
FDP_RIP.1/bArray	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_SAS.1)	FAU_SAS.1
FDP_SDI.2/DATA	No dependencies	
FIA_ATD.1/AID	No dependencies	
FIA_UID.2/AID	No dependencies	
FIA_USB.1/AID	(FIA_ATD.1)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/JC FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
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	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No dependencies	
FAU_SAS.1	No dependencies	

Table 19SFR dependency mapping

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 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

Security Functions (SF)	Description
SF.EUICC.CRYPTO	The TOE implements RSP features as described in SGP.22. Part of the features is to support additional crypto algorithms, which are part of the services provided by the Java Card system. The algorithms in scope are: • TUAK • MILENAGE
SF.EUICC.SECDOM	The TOE implements RSP features as described in SGP.22. This implementation is an extension from the features implemented according [GPCS] and grouped in **SF.GP.CM**. Extended features provide support for Profile management: • Profile downloading • Profile elements installation • Profile deletion • Profile management (enable/disable) The **SF.GP.CM** enforces the use of secure channel protocols to provide authentication and integrity and confidentiality features for data being transmitted. Additionally, specific roles are considered in the form of ECASD, ISDR, ISDP and PPR.
SF.EUICC.SCP	The TOE implements RSP features as described in SGP.22. Part of these features is support for additional secure protocol channels which are part of the services provided by the TOE. The SCP in scope are: • ES6 • ES8+ • ES10a • ES10b • ES10c

Table 20 eUICC security functions

8.2 Runtime Environment security functions

Security Functions (SF)	Description
SF.JC.FW	The TOE is based on a Java Card system as defined in [JCRE3]. Java Card provides isolation of user spaces by means of a firewall.
SF.JC.RIP	The TOE is based on a Java Card system as defined in [JCAPI3], [JCRE3] and [JCVM3]. The Java Card system provides a number features of to guarantee information from different sources made unavailable after destruction. A list of type of data and feature is listed below: • Objects: Garbage Collector • Transient data: Logical channels • Persistent data: Transaction mechanism • Packages/CAP files: Card Manager • Keys: Cryptographic containers
SF.JC.CRYPTO	The TOE is based on a Java Card system as defined in [JCAPI3]. And it provides a number of API which links to cryptographic support (key management, cryptographic operations, etc.) and PIN features. The cryptographic algorithms (supported but not in scope as a service) are AES, T-DES, ECKA, ECDSA, EC KeyGen, SHA-256, and HMAC. Nevertheless, these algorithms will provide support to **SF.GP.SCP** and **SF.EUICC.SCP**.
SF.JC.ROLLBACK	The TOE is based on a Java Card system as defined in [JCRE3]. Java Card provides features to provide atomic operation in the context of a transaction. For these operations, recovery of data is warrantied with rollback and roll forward operations.
SF.GP.CM	The TOE implements GlobalPlatform as defined in [GPCS]. The implementation include an application that provides functionalities to manage Java Card applets, including: • Packages/CAP downloading • Packages/CAP elements installation • Packages/CAP deletion The card manager enforces the use of secure channel protocols to provide authentication and integrity and confidentiality features for data being transmitted. Additionally, specific roles are considered in the form of ISD and SSD.
SF.GP.SCP	The TOE implements GlobalPlatform as defined in [GPCS]. The card manager enforces the use of secure channel protocols to provide authentication and integrity and confidentiality features for data being transmitted. The SCP in scope are: • SCP02 • SCP03 • SCP03t • SCP80 • SCP81 (TLS_PSK_WITH_AES_128_CBC_SHA256)

Table 21 Runtime Environment security functions

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 Functions (SF)	SFR Mapping Rationale
SF.EUICC.CRYPTO	FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network and FCS_CKM.4/Mobile_network
SF.EUICC.SECDOM	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FIA_UID.1/MNO-SD, FIA_USB.1/MNO-SD, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FPT_FLS.1/Platform_services, FDP_SDI.1, FPT_FLS.1, FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/PPR, FMT_MSA.1/CERT_KEYS, FMT_SMF.1, FMT_SMR.1, FMT_MSA.1/RAT, FMT_MSA.3, FIA_UID.1/EXT, FIA_UAU.1/EXT, FIA_USB.1/EXT, FIA_UAU.4/EXT, FIA_ATD.1 and FIA_API.1.1
SF.EUICC.SCP	FDP_IFC.1/SCP, FDP_IFF.1/SCP, FTP_ITC.1/SCP, FDP_ITC.2/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.4/SCP-SM and FCS_CKM.4/SCP-MNO.

Table 22 eUICC SFRs coverage

8.3.2 Runtime Environment SFRs coverage

Security Functions (SF)	SFR Mapping Rationale
SF.JC.FW	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JC, FMT_SMR.1/JC, FDP_ROL.1/FIREWALL, FMT_MTD.1/JCRE and FMT_MTD.3/JCRE.
SF.JC.RIP	FDP_RIP.1/OBJECTS, FDP_RIP.1/APDU, FDP_RIP.1/bArray, FDP_RIP.1/GlobalArray, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT and FDP_RIP.1
SF.JC.CRYPTO	FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/ECKA, FCS_COP.1/ECDSA, FCS_COP.1/HASH, FCS_COP.1/HMAC, FPR_UNO.1, FCS_RNG.1 and FPT_EMS.1.
SF.JC.ROLLBACK	FDP_RIP.1/ABORT, FPT_RCV.3/OS, FPT_RCV.4/OS
SF.GP.CM	FAU_ARP.1, FDP_SDI.2/DATA, FPT_FLS.1, FPT_TDC.1FIA_ATD.1/AID, FIA_UID.2/AID, FIA_USB.1/AID, FDP_ITC.2/Installer, FMT_SMR.1/Installer, FPT_FLS.1/Installer, FPT_RCV.3.1/Installer, FPT_FLS.1/ADEL, FDP_ACC.2/ADEL, FDP_ACF.1/ADEL, FDP_RIP.1/ADEL, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL, FDP_RIP.1/ODEL, FPT_FLS.1/ODEL, FIA_UAU.1/GP, FIA_UAU.4/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FAU_SAS.1, FMT_SMF.1/CM, FMT_SMR.1/CM, FMT_MSA.1/CM, FMT_MSA.3/CM and FCO_NRO.2/CM,
SF.GP.SCP	FMT_SMF.1/CM, FCO_NRO.2/CM, FDP_IFC.2/CM, FDP_IFF.1/CM, FDP_UIT.1/CM, FIA_UID.1/GP, FMT_MSA.1/CM, FMT_MSA.3/CM, FTP_ITC.1/CM and FMT_SMR.1/CM

Table 23 Runtime Environment SFRs coverage

9 Statement of Compatibility

The current TOE is a composite product relaying on a certified undelaying platform. This platform is a chipset compliant to [PP-84] and identified with Cert-ID: **BSI-DSZ-CC-1025-V6**.

The statement of compatibility has taken Threats, OSP, Assumptions and Objectives and Requirements from the applicable ST as identified by Cert-ID

9.1 Statement of compatibility – ASE_SPD

Threats	Rationale
T.Phys-Manipulation	Covered by IC evaluation
T.Phys-Probing	Considered during TOE evaluation
T.Malfunction	Considered during TOE evaluation
T.Leak-Inherent	Considered during TOE evaluation
T.Leak-Forced	Covered by IC evaluation
T.Abuse-Func	Considered during TOE evaluation
T.RND	Covered by IC evaluation
T.Masquerade_TOE	Covered by IC evaluation
T.Mem-Access	Considered during TOE evaluation
T.Open_Samples_Diffusion	Considered during TOE evaluation

Table 24Threats

OSP	Rationale
P.Process-TOE	Covered by IC evaluation
P.Add-Functions	Considered during TOE evaluation
P.Lim_Block_Loader	Considered during TOE evaluation
P.Ctrl_Loader	Considered during TOE evaluation
P.Crypto-Service	Considered during TOE evaluation

Table 25 OSP

Assumptions	Rationale
A.Process-Sec-IC	Considered during TOE evaluation
A.Resp-Appl	Considered during TOE evaluation
A.Key-Function	Considered during TOE evaluation

Table 26 Assumptions

9.2 Statement of compatibility – ASE_OBJ

O.TOE	Rationale
O.Phys-Manipulation	Considered during TOE evaluation
O.Phys-Probing	Considered during TOE evaluation
O.Malfunction	Considered during TOE evaluation
O.Leak-Inherent	Considered during TOE evaluation
O.Leak-Forced	Covered by IC evaluation
O.Abuse-Func	Considered during TOE evaluation
O.Identification	Considered during TOE evaluation

O.TOE	Rationale
O.RND	Covered by IC evaluation
O.Cap_Avail_Loader	Considered during TOE evaluation
O.Authentication	Considered during TOE evaluation
O.Ctrl_Auth_Loader	Considered during TOE evaluation
O.TDES	Covered by IC evaluation
O.AES	Covered by IC evaluation
O.Add-Functions	Covered by IC evaluation
O.Mem Access	Considered during TOE evaluation
O.Prot_TSF_Confidentiality	Considered during TOE evaluation

Table 27 O.TOE

O.ENV	Rationale
OE.Lim_Block_Loader	Considered during TOE evaluation
OE.TOE_Auth	Considered during TOE evaluation
OE.Loader_Usage	Considered during TOE evaluation
OE.Resp-Appl	Considered during TOE evaluation

Table 28 O.ENV

9.3 Statement of compatibility – ASE_REQ

The SFR are categorized according the following types:

- IP_SFR: Irrelevant and not used by current TOE
- RP_SFR-SERV: Relevant and used by current TOE to implement a Security Service with associated TSFI.
- RP_SFR-MECH: Relevant and used by current TOE to implement a Security Mechanism and addressed in ADV_ARC.

SFR	Rationale
FDP_ACC.1	RP_SFR-SERV
FDP_ACF.1	RP_SFR-SERV
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	RP_SFR-MECH
FDP_SDI.2	RP_SFR-MECH
FPT_PHP.3	RP_SFR-MECH
FDP_ITT.1	RP_SFR-SERV
FPT_ITT.1	IP_SFR
FDP_IFC.1	RP_SFR-SERV
FCS_RNG.1/TRNG	RP_SFR-SERV
FCS_RNG.1/HPRG	IP_SFR

SFR	Rationale
FCS_RNG.1/DRNG	RP_SFR-SERV
FCS_RNG.1/KSG	IP_SFR
FMT_LIM.1/Loader	IP_SFR
FMT_LIM.2/Loader	IP_SFR
FIA_API.1	IP_SFR
FTP_ITC.1	IP_SFR
FDP_UCT.1	IP_SFR
FDP_UIT.1	IP_SFR
FDP_ACC.1/Loader	IP_SFR
FDP_ACF.1/Loader	IP_SFR
FCS_COP.1/TDES	RP_SFR-SERV
FCS_COP.1/TDSCL	IP_SFR
FCS_COP.1/AES	RP_SFR-SERV
FCS_COP.1/AESCL	IP_SFR
FCS_COP.1/CMAC	RP_SFR-SERV
FCS_COP.1/RMAC	IP_SFR
CS_COP.1/RSA-1	IP_SFR
FCS_COP.1/RSA-2	IP_SFR
FCS_COP.1/RSA-3	IP_SFR
FCS_COP.1/ECDSA-1	RP_SFR-SERV
FCS_COP.1/ECDSA-2	RP_SFR-SERV
FCS_COP.1/ECDSA-3	RP_SFR-SERV
FCS_COP.1/ECDH-1	RP_SFR-SERV
FCS_COP.1/ECDH-2	RP_SFR-SERV
FCS_COP.1/ECDH-3	RP_SFR-SERV
FCS_COP.1/CCL	IP_SFR
FCS_CKM.1/RSA-1	IP_SFR
FCS_CKM.1/RSA-2	IP_SFR
FCS_CKM.1/RSA-3	IP_SFR
FCS_CKM.1/EC-1	RP_SFR-SERV
FCS_CKM.1/EC-2	RP_SFR-SERV
FCS_CKM.1/EC-3	RP_SFR-SERV
FCS_CKM.1/CCL	IP_SFR
FCS_CKM.4/TDES	RP_SFR-SERV
FCS_CKM.4/AES	RP_SFR-SERV
FCS_CKM.4/CCL	IP_SFR
FMT_MSA.1	RP_SFR-SERV
FMT_MSA.3	RP_SFR-SERV
FMT_SMF.1	RP_SFR-SERV
FPT_TST.2	IP_SFR

Table 29 SFR