

Kigen Consumer & IoT eUICC with LPAe/IPAe (ETu22) Security Target

Version 1.7
30 July 2026



1 Security Target Introduction	5
1.1 Security Target reference	5
1.2 TOE reference	5
1.3 References.....	5
2 TOE overview	9
2.1 TOE description	9
2.2 TOE type and usage	10
2.3 TOE lifecycle	10
2.4 Non-TOE HW/SW/FW available to the TOE.....	13
2.4.1 TOE interfaces	13
2.4.2 Description of Non-TOE HW/FW/SW and systems	14
2.5 TOE scope.....	16
2.5.1 Physical scope.....	16
2.5.2 Logical scope	17
3 Conformance Claim.....	18
3.1 Common Criteria version and conformance with CC part 2 and 3	18
3.2 Assurance package	18
3.3 Protection Profile (PP) conformance claim	18
3.4 Conformance claim rationale	18
3.4.1 Conformity of the TOE Type.....	19
3.4.2 SPD Consistency.....	19
3.4.3 Security Objectives Consistency.....	23
3.4.4 Conformity of the Requirement (SFR/SAR)	25
3.4.5 Refinements regarding Architectural design (ADV_ARC.1)	32
4 Security Problem definition	33
4.1 Assets	33
4.2 Users and Subjects	33
4.3 Threats.....	33
4.4 Organizational Security Policies	35
4.5 Assumptions.....	35
5 Security Objectives	36
5.1 Security Objectives for the TOE.....	36
5.2 Security Objectives for the Operational Environment	37
5.3 Security Objectives Rationale	37
5.3.1 Threats	37
5.3.2 Organizational Security Policies.....	44
5.3.3 Assumptions.....	44

5.3.4 Rationale Tables	44
6 Extended Components Definition.....	51
7 Security Functional requirements	52
7.1 eUICC Security Functional Requirements.....	52
7.1.1 Identification and authentication.....	52
7.1.2 Communication.....	54
7.1.3 Security Domains.....	56
7.1.4 Platform Services.....	58
7.1.5 Security management.....	59
7.1.6 Mobile Network authentication	61
7.2 LP Ae Security Functional Requirements.....	62
7.2.1 Identification and authentication.....	62
7.2.2 Communication.....	63
7.2.3 Security management.....	65
7.3 IP Ae Security Functional Requirements.....	66
7.3.1 Identification and authentication.....	66
7.3.2 Communication.....	67
7.3.3 Security management.....	70
7.4 Runtime Environment Security Requirements	70
7.4.1 CoreLG Security Functional requirements	70
7.4.2 INSTG Security Functional requirements.....	75
7.4.3 ADELG Security Functional Requirements	76
7.4.4 RMIG Security Functional Requirements.....	77
7.4.5 ODELG Security Functional Requirements	77
7.4.6 CARG Security Functional Requirements.....	77
7.4.7 Card Content Management Security Functional requirements	80
7.5 Underlying platform IC Security Functional Requirements	80
7.6 OS Update Functional Requirements.....	81
7.6.1 OS Update.....	81
7.7 Security Functional Requirements Rationale.....	83
7.7.1 SFRs for eUICC rationale.....	83
7.7.2 SFRs for LP Ae rationale.....	83
7.7.3 SFRs for IP Ae rationale	83
7.7.4 SFRs for Runtime Environment rationale.....	83
7.7.5 SFRs for OS Update rationale.....	84
7.7.6 SFRs for Underlying platform IC rationale	86
7.8 Security Functional Requirements Dependencies.....	86
7.8.1 Dependencies for eUICC SFRs	86
7.8.2 Dependencies for LP Ae SFRs	86
7.8.3 Dependencies for IP Ae SFRs.....	86
7.8.4 Dependencies for Runtime Environment SFRs	86

7.8.5 Dependencies for OS Update SFRs	87
7.8.6 Dependencies for Underlying platform IC SFRs	87
8 Statement of Compatibility	89
8.1 IC reference.....	89
8.2 Security Objectives Consistency.....	89
8.3 Security Objectives for the Environment Consistency	91
8.4 Security Functional Requirements Consistency.....	91
9 TOE Summary Specification	94
9.1 eUICC security functions.....	94
9.2 Runtime Environment security functions	95
9.3 OS Update security functions	96
9.4 TSS Rationale	97
9.4.1 eUICC SFRs coverage	97
9.4.2 Runtime Environment SFRs coverage.....	97
9.4.3 OS Update SFRs coverage.....	98

1 Security Target Introduction

1.1 Security Target reference

Name	Kigen Consumer & IoT eUICC with LP Ae/IP Ae (ETu22) Security Target
Version	1.7
Reference	KIGEN-eUICC-17 (ETu22)

Table 1 Security Target Reference

1.2 TOE reference

Name	Kigen Consumer & IoT eUICC (ETu22)
Version	2.0
Reference	KIGEN-eUICC-20 (ETu22)

Table 2 TOE Reference

1.3 References

Ref	DocNumber	Title	Version
[1]	[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model	CC:2022 Revision 1, November 2022
[2]	[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components	CC:2022 Revision 1, November 2022
[3]	[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components	CC:2022 Revision 1, November 2022
[4]	[PP-eUICC]	eUICC for Consumer and IoT Devices Protection Profile	Version 2.1, 3 February 2025
[5]	[PP-JCS]	Java Card System – Open Configuration Protection Profile	Version 3.1, April 2020
[6]	[PP-GP]	GlobalPlatform – 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

Ref	DocNumber	Title	Version
[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.	Release 11
[18]	[TUAK]	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0, release 12, December 2014. · Document 1: Algorithm specification; · Document 2: Implementers' test data; · Document 3: Design conformance test data.	Release 12
[19]	[SGP.22]	Remote SIM Provisioning (RSP) Technical Specification, version: 2.6.1, GSM Association, April 2025. 2.7, GSM Association, April 2026.	v2.6.1 and v2.7
[20]	[SGP.32]	eSIM IoT Technical Specification, version: 1.2, GSM Association, June 2024. 1.3, GSM Association, May 2026.	v1.2 and v1.3

Ref	DocNumber	Title	Version
[21]	[CC-5]	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements	CC:2022 Revision 1, November 2022.
[22]	[IC_CERT_REPORT]	BSI-DSZ-CC-1272-2026 for IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite	BSI-DSZ-CC-1272-2026, EUCC-3087-2026-02-0001
[23]	[IC_ST]	IFX_CCI_00007Ah/8Fh A11/R11/M11 with optional Crypto Suite Security Target Lite	Rev 1.0, 2025-10-16
[24]	[Guidances]	- Kigen OS Operating System Reference Manual - v1.44 - Kigen OS eUICC HTTPS and CoAP Applet Reference Manual - v3.3 - Kigen OS eUICC ISD-A and ISD-R Applets Reference Manual -v1.11 - Kigen OS eUICC Patch Mechanism Reference Manual - v1.8 - Kigen OS eUICC Profile Format Reference Manual - v1.5 - Kigen OS eUICC Personalization Reference Manual - v1.14 - Kigen OS eUICC Security Domains Reference Manual - v1.25 - Kigen OS eUICC USIM Applet Reference Manual - v1.8 - Kigen OS eUICC IP Ae Reference Manual - v1.5 - Kigen OS eUICC In-Factory Personalisation Process Reference Manual – 1.2 - Kigen eUICC OS Release ETu22.05 Data Sheet for Supported Microcontrollers - Kigen OS Release Package for ETu22 User Guide – v0.4 - Kigen proprietary eUICC API (com.kigen.eUiccApi) Javadoc documentation - eUiccApi_v1.5.zip - Kigen proprietary API kigenApi1 (com.kigen.kigenApi1) Javadoc documentation - kigenApi1_v2.2.zip - Kigen Recommendations and User Guidance – v1.5 - GlobalPlatform Card Composition Model Security Guidelines for Basic Applications Version 2.0, GPC_GUI_050	The version is indicated next to each document.

Ref	DocNumber	Title	Version
[25]	[PP-117]	Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile	Version 1.8, 26 October 2023
[26]	[Infineon_Guidances]	32-bit Security Controller - V31 Security guidelines Revision 1.00-3076 2025-04-30 - CS-SLC22V31 CryptoSuite - 32-bit Security Controller - User interface manual - Version 5.02.003 2025-10-02 - Preliminary Production and personalization manual, Z8F80801257-A	Indicated next to the title of each document

Table 3 References

2 TOE overview

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

2.1 TOE description

The TOE Kigen Consumer & IoT eUICC (ETu22) Version 2.0 is an eUICC that implements:

- GSMA RSP Technical Specification [19] for Consumer Devices.
- GSMA eSIM IoT Technical Specification [20] for IoT Devices.

The TOE follows an architecture as depicted below:

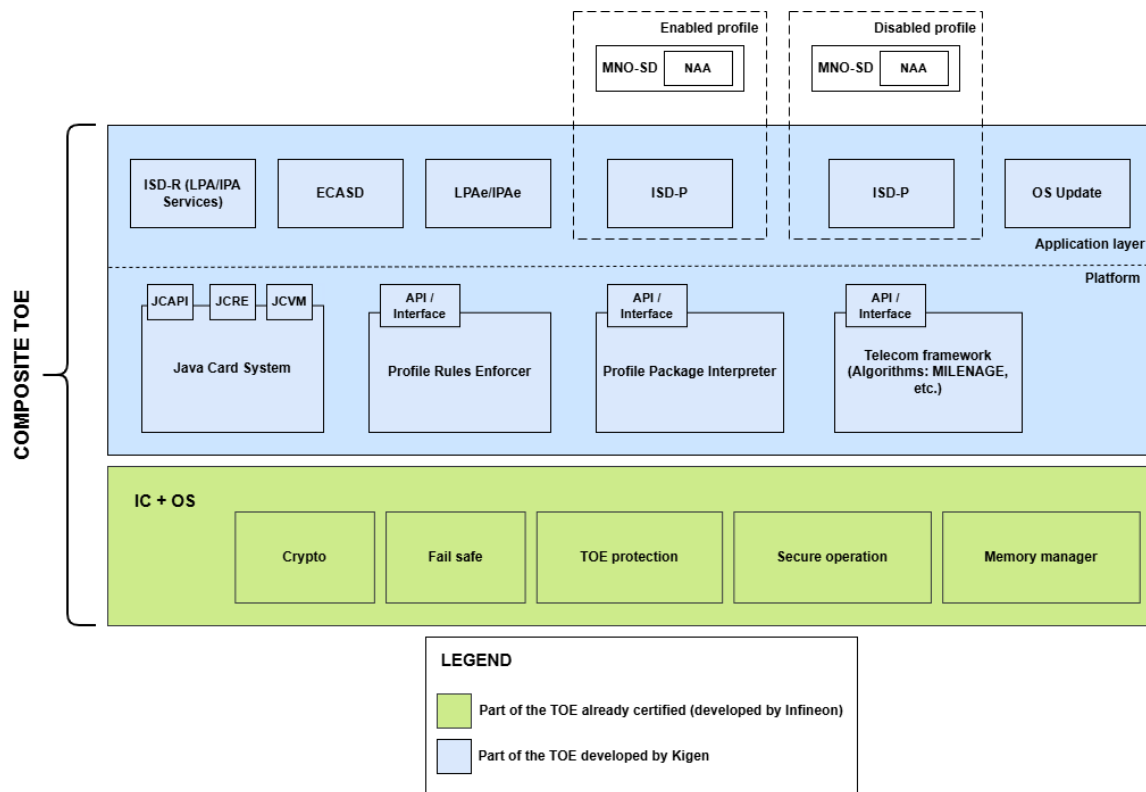


Figure 1: TOE Architecture

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/IPA 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.
 - An LPAe, same functions as the (optional) non-TOE on-device unit LPA_d.
 - An IPAe, same functions as the (optional) non-TOE on-device unit IPA_d.
- 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.
 - A Global Platform Card Manager built to card management.
- Runtime Environment: Operating System implemented built on top of an Integrated Circuit providing support to the applets.
- OS Update: eUICC OS Update capability.
- Hardware IC with the corresponding firmware.

The TOE is developed by two different entities: Infineon and Kigen. Kigen is the actor responsible for developing the specific eUICC software, while Infineon develops the IC already certified.

The Profiles are not part of the TOE neither the Local User Interface (LUI_e).

2.2 TOE type and usage

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

An eUICC with an enabled operational Profile provides the same functionality as a UICC.

Additionally, the eUICC incorporates an LPAe, providing the LPDe (local profile download) and LDSe (local discovery service) features. Also, the eUICC incorporates an IPAe, providing the Profile Download, the Discovery Service, the Notification Handling, Conveying eIM Packages and related results.

The LPAe (except LUI_e, which is not implemented in the TOE) and IPAe are implemented as part of the ISD-R. The LPAe and the IPAe can use the eUICC Rules Authorisation Table (RAT) to determine whether or not a Profile containing Profile Policy Rules (PPRs) is authorised to be installed on the eUICC.

The eUICC can be hosted in either a Consumer or IoT Device.

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

2.3 TOE lifecycle

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

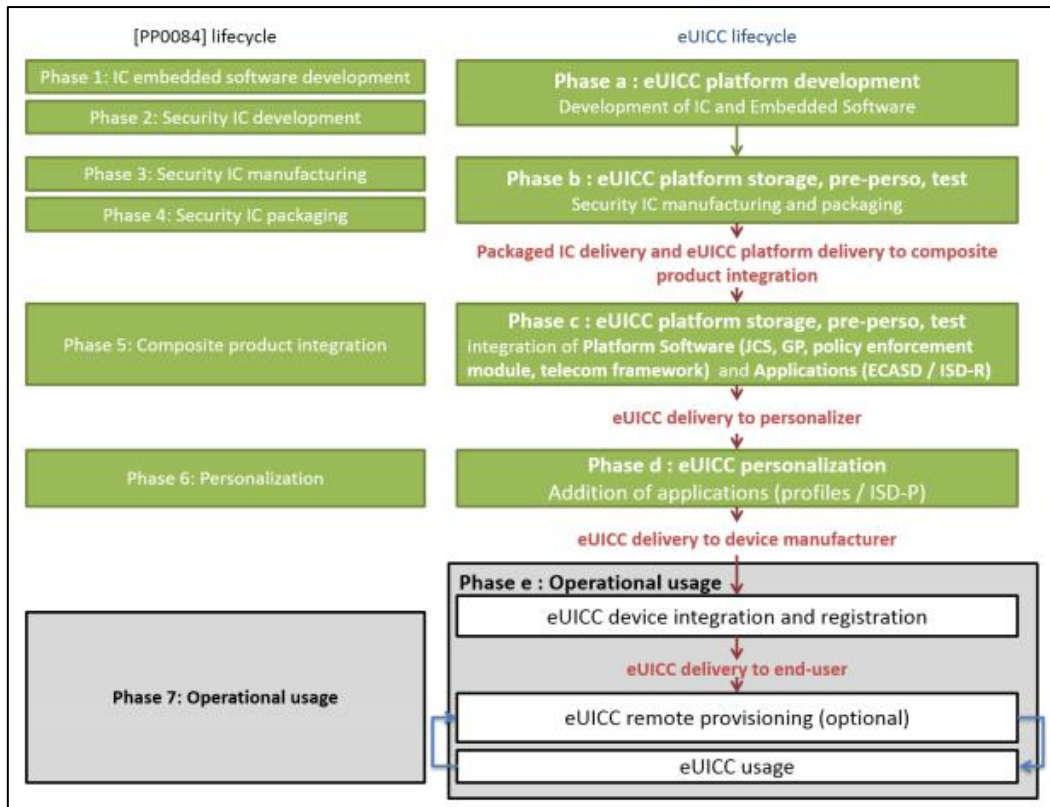


Figure 2 TOE Life Cycle

The reader may refer to [2] 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, 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:** eUICC Platform 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.
 - TOE Delivery [optional]: At this phase the delivery of the TOE could happen, if the TOE is already self-protected;
- **Phase c:** eUICC platform storage, pre-personalization, test covers the stage of the embedding of software products onto the eUICC.
 - TOE Delivery [optional]: At this phase the delivery of the TOE could happen, if the TOE is already self-protected except in case the Phase c and Phase d (GSMA SAS) are performed at the same secure site in which case the eUICC Manufacturer is considered as trusted administrator to enable the TOE self-protection before the end of phase d;
- **Phase d:** eUICC personalization covers the ECASD /ISD-R keys and optionally the addition of provisioning Profiles and Operational Profiles onto the eUICC.

- TOE Delivery [optional]: *At this phase the delivery of the TOE to the customer of the eUICC manufacturer happens at the latest;*
- **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 the protection profile SGP.25 [4].

The TOE is self-protected at the end of phase b. The delivery of the TOE also happens at the end of phase b.

The TOE life cycle is composed of the following stages:

Phase	Site	Actions
Phase a	Kigen's sites in Copenhagen and United Kingdom (Sites with Reference Number SALN0077)	OS Development and native applets Pre-personalisation data preparation
	(Sites covered by the IC certificate [ICs_CERT_REPORT])	Development of IC and IC dedicated Software
Phase b	Kigen's partner. Sites covered by the IC certificate [ICs_CERT_REPORT] (Global Foundries fab 7 in Singapore, DHL Singapore, KWE Shanghai and K&N Großostheim).	Test cover the stages related to manufacturing IC pre-personalisation TOE is self-protected
TOE DELIVERY		
Phase c	Kigen's partner	OS installation (integration), native applet installation Pre-personalisation
Phase d	Kigen's partner	Personalization
Phase e	Kigen Customer / partner	Personalization, profile installation (depending on final customer needs)

Table 4 Lifecycle

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

2.4.1 TOE interfaces

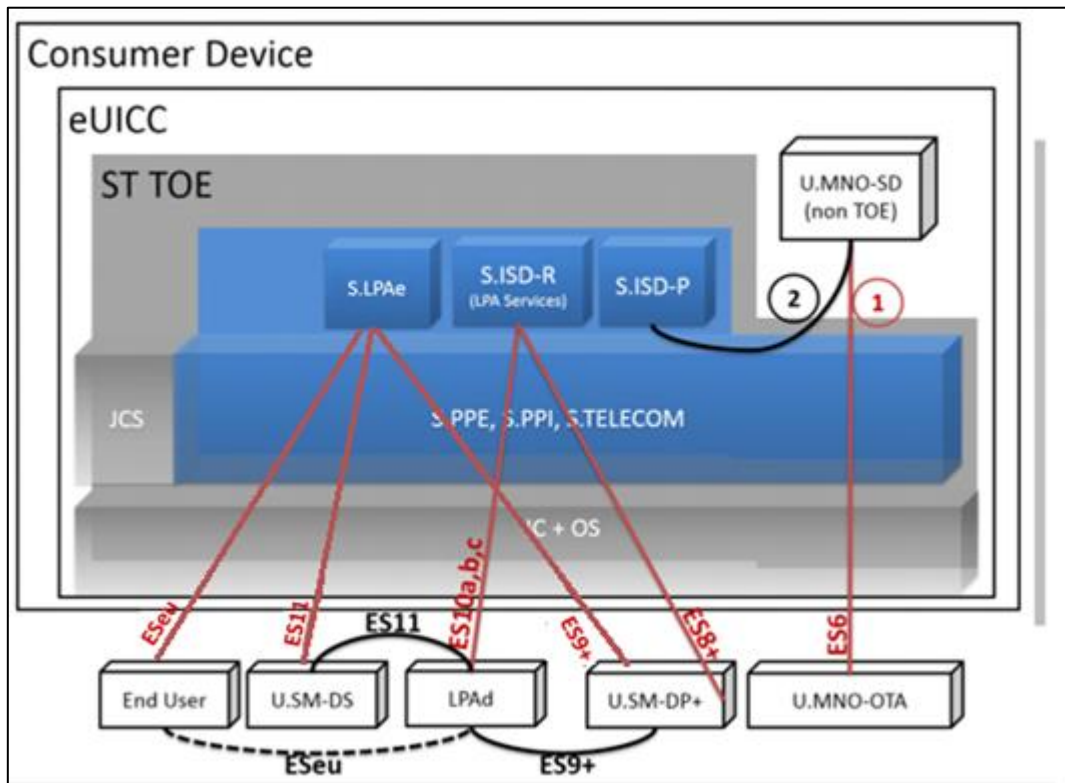


Figure 3 TOE Interfaces with LP Ae

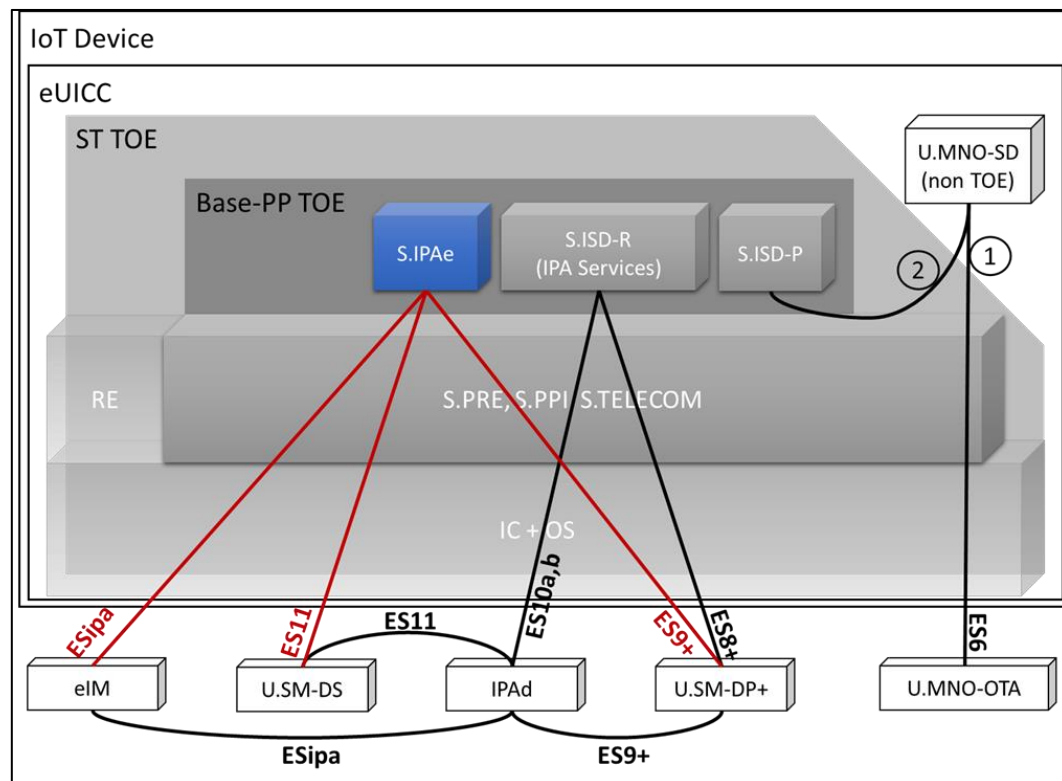


Figure 4 TOE Interfaces with IP Ae

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

- With the provisioning infrastructure, consisting in SM-DS, SM-DP+, eIM (SGP.32), and LPAd/IPAd interfaces (identified respectively ES11, ES8+/ES9+, ESep/ESipa and ES10a-c);
- 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 MNO-SD and the ISD-P.
- Important to mention that the TOE does not implement Local User Interface, instead, the TOE communicates with a necessary LPAd which implements an LUI.

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).

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

- **Device**

The eUICC is intended to be plugged in a Consumer Device or an IoT Device. This equipment can be a mobile phone, or any other connected Device.

The Consumer Device is expected to include a user interface to interact with End User. Given that LUI is not implemented by the LPAd of the TOE.

The IoT Device can be either a Network Constrained Device or a User Interface Constrained Device.

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.

- **JavaCard**

- Java Card system; including the JCVM [7], JCAPI [8] and JCRE [9]. Features are implemented natively, JavaCard is not in the scope of this ST.

- **MNO-SD and applications**

The Profile controlled by each ISD-P consists in an 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.

The TOE communicates with remote servers of:

- SM-DS, which provides mechanisms for discovery of SM-DP+s;
- SM-DP+, which provides Platform and Profile management commands as well as Profiles.
- eIM, which is responsible for remote Profile State Management Operations (PSMO) and eIM Configuration Operations (eCO) on a single IoT Device or a fleet of IoT Devices.

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 root of trust called the eSIM CA, whose public key is stored pre-issuance on the eUICC.

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

- **Bytecode verifier**

Bytecode verifier (BCV) must be used before loading a new applet (developed following the rules defined in [GPC-Gui]) in phase e of the TOE life cycle, which is considered as not part of the TOE.

The TOE does not implement the RMI functions from JCS.

The Profiles are not part of the TOE.

2.5 TOE scope

2.5.1 Physical scope

The TOE Kigen Consumer & IoT eUICC (ETu22) is composed by the following components:

Category	Component	Version	Delivery form	Delivery method
HW	IC Hardware	IFX_CCI_00007Ah A11 IFX_CCI_00007Ah M11 IFX_CCI_00007Ah R11 [IC_CERT_REPORT]	IC case Package other	Physical delivery
FW	BOS	80.510.04.03	Binary file in memory	Embedded on the IC
FW	Flash-loader	10.09.0000	Binary file in memory	Embedded on the IC
SW	HSL	04.07.0000	Object files	Secure download via iShare
SW	UMSLC	02.01.0040	Object files	Secure download via iShare
SW	Crypto Suite	5.02.003	Object files	Secure download via iShare
SW	Kigen ETu22	05	Binary file in flash loader command file format	Delivered ciphered - email or other file transfer method
DOC	Kigen eUICC guidances	[Guidances]	PDF	Delivered ciphered - email or other file transfer method
DOC	Infineon guidances	[Infineon_Guidances]	PDF	Secure download via iShare

Table 5 Physical scope

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.
 - An LPAe, same functions as the (optional) non-TOE on-device unit LPAd.
 - An IPAe, same functions as the (optional) non-TOE on-device unit IPAd.
- 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:
 - GlobalPlatform system; including Card Content Management system [11].
 - Native system; including Cryptographic primitives, Memory management and Communication protocol management.
- OS Update: eUICC OS Update capability.
- Hardware IC with the corresponding firmware.

The Java API is considered outside the scope of this evaluation as a service for third-party applets and it is included in the scope of the evaluation only for the functionalities required by the eUICC.

3 Conformance Claim

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

This Security Target is conformant to Common Criteria 2022 release 1, taking into account version 1.2 of Errata and Interpretation for CC:2022 Revision 1 (CCMB-2022-11-006).

This Security Target is conformant to:

- CC Part 1 [CC-1],
- CC Part 2 [CC-2] (extended),
- CC Part 3 [CC-3] (conformant),
- CC Part 5 [CC-5].

3.2 Assurance package

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 and the composite product package (COMP).

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

3.3 Protection Profile (PP) conformance claim

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

The TOE claims conformance to the IPAe PP-configuration detailed in section 10 of [PP-eUICC]. Furthermore, the Security Target is based on LPAe PP-module (LUIe is not implemented), explained in section 8 of [PP-eUICC].

As the TOE implements the OS Update functionality, the PP Module OS Update (stated in Annex A of [PP-eUICC]) is applied in the current evaluation.

3.4 Conformance claim rationale

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

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

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

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].

In addition to the above conformance claim rationale, the following notation is added to clarify the specific configuration by which the requirement, SPD element or security objectives is added.

- Those requirements, SPD elements or security objectives performed that contains between parenthesis SGP.22 (like "(SGP.22)") are addressed exclusively to Consumer Device configuration.
- Those requirements, SPD elements or security objectives performed that contains between parenthesis SGP.32 (like "(SGP.32)") are addressed exclusively to IoT configuration.
- Those requirements, SPD elements or security objectives performed that do not contain a previous indication, are addressed to both configurations.

3.4.1 Conformity of the TOE Type

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

The TOE follows the third scenario from the definition in [PP-eUICC] when the embedded eUICC is embedded in a certified IC, but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs 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.

Assets	PP-eUICC	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_RULES	X	(E)
D.PROFILE_USER_CODES (SGP.22)	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)
D.PK.EIM.ECDSA (SGP.32)	X	(E)
D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)

D.CRLs	X	(E)
D.APP_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.LPAe_TSF_CODE	X	(E): as part of LP Ae PP-module
D.LPAe_DEVICE_INFO	X	(E): as part of LP Ae PP-module
D.LPAe_KEYS	X	(E): as part of LP Ae PP-module
D.IP Ae_TSF_CODE	X	(E): as part of IP Ae PP-module
D.IP Ae_DEVICE_INFO	X	(E): as part of IP Ae PP-module
D.IP Ae_KEYS	X	(E): as part of IP Ae PP-module
D.UPDATE_IMAGE	X	(E): as part of OS Update PP-module
D.TOE_IDENTIFIER	X	(E): as part of OS Update PP-module
D.OS-UPDATE_KEY(S)	X	(E): as part of OS Update PP-module

Table 6 Assets Consistency

3.4.2.2 Users, Subjects and Security Aspects 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-DP+	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.eIM (SGP.32)	X	(E)
U.End-User (SGP.22)	X	(E)

Table 7 User Consistency

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

Security Aspect	PP-eUICC	Security Target
SA.CONFID-UPDATE-IMAGE	X	(E): as part of OS Update PP-module
SA.INTEG-UPDATE-IMAGE	X	(E): as part of OS Update PP-module

Table 8 Security Aspects Consistency

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

Subjects	PP-eUICC	Security Target
S.ISD-R	X	(E)
S.ISD-P	X	(E)
S.EC ASD	X	(E)
S.PPI	X	(E)
S.PRE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A): Added from [PP-JCS].
S.APPLET		(A): Added from [PP-JCS].
S.BCV		(A): Added from [PP-JCS].
S.CAD		(A): Added from [PP-JCS].
S.SD		(A): Added from [PP-JCS].
S.INSTALLER		(A): Added from [PP-JCS].
S.JCRE		(A): Added from [PP-JCS].
S.JCVM		(A): Added from [PP-JCS].
S.LOCAL		(A): Added from [PP-JCS].
S.MEMBER		(A): Added from [PP-JCS].
S.CAP_FILE		(A): Added from [PP-JCS].
S.LPAe	X	(R): Part of LPAe PP-module and refined since LU1e is not implemented in the TOE
S.IP Ae	X	(E): as part of IP Ae PP-module
S.OSU	X	(E): as part of OS Update PP-module
S.UpdateImageCreator	X	(E): as part of OS Update PP-module

Table 9 Subjects Consistency

3.4.2.3 Threats consistency

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

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

T.UNAUTHORIZED-IDENTITY-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.IDENTITY-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-eUICC	X	(E)
T.LPAd-INTERFACE-EXPLOIT	X	(E)
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)
T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)
T.PLATFORM-MNG-INTERCEPTION-LPDe	X	(R): Part of LP Ae PP-module and refined since LUIe is not implemented in the TOE
T.PLATFORM-MNG-INTERCEPTION-LDSe	X	(E): as part of LP Ae PP-module
T.UNAUTHORIZED-PLATFORM-MNG-LP Ae	X	(R): Part of LP Ae PP-module and refined since LUIe is not implemented in the TOE
T.PROFILE-MNG-ELIGIBILITY-LP Ae	X	(E): as part of LP Ae PP-module
T.LOGICAL-ATTACK-LP Ae	X	(R): Part of LP Ae PP-module and refined since LUIe is not implemented in the TOE
T.PHYSICAL-ATTACK-LP Ae	X	(R): Part of LP Ae PP-module and refined since LUIe is not implemented in the TOE
T.PLATFORM-MNG-INTERCEPTION-IP Ae	X	(E): as part of IP Ae PP-module
T.UNAUTHORIZED-PLATFORM-MNG-IP Ae	X	(E): as part of IP Ae PP-module
T.PROFILE-MNG-ELIGIBILITY-IP Ae	X	(E): as part of IP Ae PP-module
T.LOGICAL-ATTACK-IP Ae	X	(E): as part of IP Ae PP-module
T.PHYSICAL-ATTACK-IP Ae	X	(E): as part of IP Ae PP-module
T.CONFID-UPDATE-IMAGE.LOAD	X	(E): as part of OS Update PP-module
T.INTEG-UPDATE-IMAGE.LOAD	X	(E): as part of OS Update PP-module
T.UNAUTH-UPDATE-IMAGE.LOAD	X	(E): as part of OS Update PP-module
T.INTERRUPT_OSU	X	(E): as part of OS Update PP-module

Table 10 Threats Consistency

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 11 Organizational Security Policies Consistency

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-IPAd	X	(E)
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.CAP_FILE		(A): Added from [PP-JCS]
A.VERIFICATION		(A): Added from [PP-JCS]
A.ACTORS-LPAe	X	(E): as part of LPAe PP-module
A.ACTORS-IP Ae	X	(E): as part of IP Ae PP-module
A.Process-Sec-IC		(A): Added from [PP-84]

Table 12 Assumptions Consistency

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.PRE-PPI	X	(E)
O.eUICC-DOMAIN-RIGHTS	X	(E)
O.SECURE-CHANNELS	X	(E)
O.INTERNAL-SECURE-CHANNELS	X	(E)
O.PROOF_OF_IDENTITY	X	(E)
O.OPERATE	X	(E)
O.API	X	(E)
O.DATA-CONFIDENTIALITY	X	(E)
O.DATA-INTEGRITY	X	(E)
O.ALGORITHMS	X	(E)
O.IC.PROOF_OF_IDENTITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.IC.SUPPORT		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment

O.IC.RECOVERY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.PRE-PPI		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.SECURE-COMM		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.API		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.DATA-CONFIDENTIALITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.DATA-INTEGRITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.IDENTITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.RE.CODE-EXE		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment
O.SECURE-CHANNELS-LPAe	X	(E): as part of LP Ae PP-module
O.INTERNAL-SECURE-CHANNELS-LPAe	X	(E): as part of LP Ae PP-module
O.DATA-CONFIDENTIALITY-LPAe	X	(E): as part of LP Ae PP-module
O.DATA-INTEGRITY-LPAe	X	(R): Part of LP Ae PP-module and refined since LUIe is not implemented in the TOE
O.SECURE-CHANNELS-IP Ae	X	(E): as part of IP Ae PP-module
O.INTERNAL-SECURE-CHANNELS-IP Ae	X	(E): as part of IP Ae PP-module
O.DATA-CONFIDENTIALITY-IP Ae	X	(E): as part of IP Ae PP-module
O.DATA-INTEGRITY-IP Ae	X	(E): as part of IP Ae PP-module
O.SECURE_LOAD_ACODE	X	(E): as part of OS Update PP-module
O.SECURE_AC_ACTIVATION	X	(E): as part of OS Update PP-module
O.TOE_IDENTIFICATION	X	(E): as part of OS Update PP-module
O.CONFID-UPDATE-IMAGE.LOAD	X	(E): as part of OS Update PP-module
O.AUTH-LOAD-UPDATE-IMAGE	X	(E): as part of OS Update PP-module

Table 13 Security objectives for the TOE Consistency

3.4.3.2 Objective for Environment consistency

O.ENV	PP-eUICC	Security Target
--------------	-----------------	------------------------

OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.MNO	X	(E)
OE.EIM (SGP.32)	X	(E)
OE.TRUSTED-PATHS-LPAd-IPAd	X	(E)
OE.APPLICATIONS	X	(E): Security Guidelines from [GPC-Gui]
OE.MNO-SD	X	(E)
OE.CAP_FILE		(A): Added from [PP-JCS].
OE.VERIFICATION		(A): Added from [PP-JCS].
OE.CODE-EVIDENCE		(A): Added from [PP-JCS].
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PRE-PPI	X	Removed and replaced by O.RE.PRE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE
OE.CONFID_UPDATE_IMAGE.CREATE	X	(E): as part of OS Update PP-module
OE.Process-Sec-IC		A: Added from [PP-84]

Table 14 Security objectives for the Operational Environment Consistency

3.4.4 Conformity of the Requirement (SFR/SAR)

3.4.4.1 SFR consistency

SFR	PP-eUICC	Security Target
<u>FIA_UID.1/EXT</u>	X	(E)
<u>FIA_UAU.1/EXT</u>	X	(E)
<u>FIA_USB.1/EXT</u>	X	(E)

<u>FIA_UAU.4/EXT</u>	X	(E)
<u>FIA_UID.1/MNO-SD</u>	X	(E)
<u>FIA_USB.1/MNO-SD</u>	X	(E)
<u>FIA_ATD.1/Base</u>	X	(E)
<u>FIA_API.1</u>	X	(E)
<u>FDP_IFC.1/SCP</u>	X	(E)
<u>FDP_IFF.1/SCP</u>	X	(E)
<u>FDP_ITC.1/SCP</u>	X	(E)
<u>FDP_ITC.2/SCP</u>	X	(E)
<u>FDP_TDC.1/SCP</u>	X	(E)
<u>FDP_UCT.1/SCP</u>	X	(E)
<u>FDP_UIT.1/SCP</u>	X	(E)
<u>FCS_CKM.1/SCP-SM</u>	X	(E)
<u>FCS_CKM.2/SCP-MNO</u>	X	(E)
<u>FCS_CKM.6/SCP-SM</u>	X	(E)
<u>FCS_CKM.6/SCP-MNO</u>	X	(E)
<u>FDP_ACC.1/ISDR</u>	X	(E)
<u>FDP_ACF.1/ISDR</u>	X	(E)
<u>FDP_ACC.1/ECASD</u>	X	(E)
<u>FDP_ACF.1/ECASD</u>	X	(E)
<u>FDP_IFC.1/Platform_services</u>	X	(E)
<u>FDP_IFF.1/Platform_services</u>	X	(E)
<u>FDP_FLS.1/Platform_services</u>	X	(E)
<u>FCS_RNG.1</u>	X	(E)
<u>FPT_EMS.1/Base</u>	X	(E)
<u>FDP_SDI.1/Base</u>	X	(E)
<u>FDP_RIP.1/Base</u>	X	(E)
<u>FPT_FLS.1/Base</u>	X	(E)
<u>FMT_MSA.1/PLATFORM_DATA</u>	X	(E)
<u>FMT_MSA.1/RULES</u>	X	(E)
<u>FMT_MSA.1/CERT_KEYS</u>	X	(E)
<u>FMT_SMF.1/Base</u>	X	(E)
<u>FMT_SMR.1/Base</u>	X	(E)
<u>FMT_MSA.1/RAT</u>	X	(E)
<u>FMT_MSA.3/Base</u>	X	(E) Refined with iteration.
<u>FCS_COP.1/Mobile_network</u>	X	(E)
<u>FCS_CKM.2/Mobile_network</u>	X	(E)

<u>FCS_CKM.6/Mobile_network</u>	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.
FCS_CKM.1/ECDH		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/SIG_ECC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/TDES		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/AES		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.6/RE		(A): Added from [PP-JCS]. Refined with iteration. FCS_CKM.4 adapted to CC2022.
FCS_COP.1/ECDH		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/MD		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/MAC_TDES		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/MAC_AES		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/SIG_ECC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/CIPH_TDES_CBC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/CIPH_AES_GCM		(A): Added from [PP-JCS]. Refined with iteration.
FCS_COP.1/CIPH_AES_CBC		(A): Added from [PP-JCS]. Refined with iteration.

FCS_COP.1/HMAC		(A): Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A): Added from [PP-JCS].
FDP_RIP.1/APDU		(A): Added from [PP-JCS].
FDP_RIP.1/bArray		(A): Added from [PP-JCS].
FDP_RIP.1/GlobalArray		(A): Added from [PP-JCS].
FDP_RIP.1/KEYS		(A): Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A): Added from [PP-JCS].
FAU_ARP.1		(A): Added from [PP-JCS].
FDP_SDI.2/DATA		(A): Added from [PP-JCS].
FPR_UNO.1		(A): Added from [PP-JCS].
FPT_FLS.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FPT_TDC.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ITC.2/Installer		(A): Added from [PP-JCS].
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/CM		(A): Added from [PP-JCS].
FMT_MSA.1/CM		(A): Added from [PP-JCS].
FMT_MSA.3/CM		(A): Added from [PP-JCS].
FMT_SMF.1/CM		(A): Added from [PP-JCS].
FMT_SMR.1/CM		(A): Added from [PP-JCS].
FTP_ITC.1/CM		(A): Added from [PP-JCS].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FMT_SMR.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 O.IC.SUPPORT.
FIA_UID.1/LPAe	X	(E): as part of LP Ae PP-module
FIA_UAU.1/LPAe	X	(E): as part of LP Ae PP-module
FIA_USB.1/LPAe	X	(E): as part of LP Ae PP-module
FIA_UAU.4/LPAe	X	(E): as part of LP Ae PP-module
FIA_ATD.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_IFC.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_IFF.1/LPAe	X	(E): as part of LP Ae PP-module
FTP_ITC.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_ITC.2/LPAe	X	(E): as part of LP Ae PP-module
FPT_TDC.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_UCT.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_UIT.1/LPAe	X	(E): as part of LP Ae PP-module
FCS_CKM.1/LPAe	X	(E): as part of LP Ae PP-module
FCS_CKM.6/LPAe	X	(E): as part of LP Ae PP-module
FPT_EMS.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_SDI.1/LPAe	X	(E): as part of LP Ae PP-module
FDP_RIP.1/LPAe	X	(E): as part of LP Ae PP-module
FMT_SMF.1/LPAe	X	(E): as part of LP Ae PP-module
FMT_SMR.1/LPAe	X	(E): as part of LP Ae PP-module
FIA_UID.1/IP Ae	X	(E): as part of IP Ae PP-module
FIA_UAU.1/IP Ae	X	(E): as part of IP Ae PP-module

FIA_USB.1/IP Ae	X	(E): as part of IP Ae PP-module
FIA_UAU.4/IP Ae	X	(E): as part of IP Ae PP-module
FIA_ATD.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_IFC.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_IFF.1/IP Ae	X	(E): as part of IP Ae PP-module
FTP_ITC.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_ITC.2/IP Ae	X	(E): as part of IP Ae PP-module
FPT_TDC.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_UCT.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_UIT.1/IP Ae	X	(E): as part of IP Ae PP-module
FCS_CKM.1/IP Ae	X	(E): as part of IP Ae PP-module
FCS_CKM.6/IP Ae	X	(E): as part of IP Ae PP-module
FPT_EMS.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_SDL.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_RIP.1/IP Ae	X	(E): as part of IP Ae PP-module
FMT_SMF.1/IP Ae	X	(E): as part of IP Ae PP-module
FMT_SMR.1/IP Ae	X	(E): as part of IP Ae PP-module
FDP_ACC.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FDP_ACF.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FIA_ATD.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FMT_MSA.3/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FMT_SMR.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FMT_SMF.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FTP_TRP.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module
FCS_COP.1/OS-UPDATE-DEC	X	(A): added from [PP-GP] to cover OS Update PP-Module
FCS_COP.1/OS-UPDATE-VER	X	(A): added from [PP-GP] to cover OS Update PP-Module
FPT_FLS.1/OS-UPDATE	X	(A): added from [PP-GP] to cover OS Update PP-Module

Table 15 Security Functional Requirement Consistency

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.

The Security Assurance Requirements for the evaluation of the TOE are those taken from

- Evaluation Assurance Level 4 (EAL4)
- Composite product package (COMP)

and augmented by taking the following components:

- ALC_DVS.2
- AVA_VAN.5

The assurance requirements are:

Class ADV: Development

Architectural design (ADV_ARC.1)

Functional specification (ADV_FSP.4)

Implementation representation (ADV_IMP.1)

TOE design (ADV_TDS.3)

Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority. (ADV_COMP.1)

Class AGD: Guidance documents

Operational user guidance (AGD_OPE.1)

Preparative user guidance (AGD_PRE.1)

Class ALC: Life-cycle support

CM capabilities (ALC_CMC.4)

CM scope (ALC_CMS.4)

Delivery (ALC_DEL.1)

Development security (ALC_DVS.2)

Life-cycle definition (ALC_LCD.1)

Tools and techniques (ALC_TAT.1)

Integration of the dependent component into the related base component and consistency check for delivery and acceptance procedures. (ALC_COMP.1)

Class ASE: Security Target evaluation

Conformance claims (ASE_CCL.1)

Extended components definition (ASE_ECD.1)

ST introduction (ASE_INT.1)

Security objectives (ASE_OBJ.2)

Derived security requirements (ASE_REQ.2)

Security problem definition (ASE_SPD.1)

TOE summary specification (ASE_TSS.1)

Consistency of Security Target (ASE_COMP.1)

Class ATE: Tests

Coverage (ATE_COV.2)

Depth (ATE_DPT.1)

Functional tests (ATE_FUN.1)

Independent testing (ATE_IND.2)

Composite product functional testing (ATE_COMP.1)

Class AVA: Vulnerability assessment

Vulnerability analysis (AVA_VAN.5)

Composite product vulnerability assessment (AVA_COMP.1).

3.4.5 Refinements regarding Architectural design (ADV_ARC.1)

The following text reflects the requirements of the selected component ADV_ARC.1 and the refinement for the ADV_ARC.1.2C:

ADV_ARC.1 Security architecture description
--

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

Refinement:

In order to enforce the domain separation, the rules included in A.APPLICATIONS must be sufficient to maintain the security for all applications loaded on the eUICC containing the TOE.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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 base PP, LP Ae PP-Module (except D.LP Ae_PROFILE_USER_CODES and D.LP Ae_PROFILE_DISPLAYED_METADATA, as LUIe is not implemented in the TOE), IP Ae PP-Module and OS Update PP-module 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 base PP, LP Ae PP-Module, IP Ae PP-Module and OS Update PP-module from [PP-eUICC] is not repeated here. See section 3.4.2.2 for complete list is users and subjects.

The description of the refined subject is detailed below:

- **S.LP Ae**
The definition of this subject has been refined as follows since LUIe is not implemented in the TOE:
The LP Ae is a functional element within the TOE that provides the LP De and LD Se features.

4.3 Threats

The definition of threats from base PP, LP Ae PP-Module, IP Ae PP-Module and OS Update PP-module 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 is 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 threatens the assets: D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT, D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYS and D.APP_CODE.
- **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.
- **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.APP_CODE and D.APP_I_DATA.
- **T.UNAUTHORIZED-IDENTITY-MNG**

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

Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, D.APP_CODE, D.APP_I_DATA, D.APP_KEYS, D.APP_C_DATA and D.PK.EIM.ECDSA (SGP.32).

- **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.PLATFORM_DATA, D.PROFILE_RULES, D.PLATFORM_RAT, D.API_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYS and D.APP_C_DATA.

- **T.UNAUTHORIZED-PLATFORM-MNG-LPAe**

The definition of this threat has been refined as follows since the LUle is not implemented in the TOE:

An on-card application:

- modifies or discloses LP Ae data;
- executes or modifies operations from LP Ae.

In particular, the following case could happen:

- the Device Information could be modified before being sent to the eUICC causing:
 - a failure of the eligibility check for a profile, or
 - a downgrade of security parameters, such as indicating that the device does not support certificate revocation lists (CRLs).

Such a threat typically includes for example:

- direct access to fields or methods of the Java objects
- exploitation of the APDU buffer and global byte array

Directly threatens the asset: D.LPAe_TSF_CODE.

- **T.PLATFORM-MNG-INTERCEPTION-LPDe**

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

Directly threatens the asset: D.LPAe_KEYS.

- **T.UNAUTHORIZED-PLATFORM-MNG-LPAe**

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

Directly threatens the asset: D.LPAe_TSF_CODE.

- **T.LOGICAL-ATTACK-LPAe**

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.LPAe_TSF_CODE, D.LPAe_DEVICE_INFO and D.LPAe_KEYS.

- **T.PHYSICAL-ATTACK-LPAe**

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.LPAe_TSF_CODE, D.LPAe_DEVICE_INFO and D.LPAe_KEYS.

4.4 Organizational Security Policies

The definition of organizational security policies from base PP, LPAe PP-Module, IPAe PP-Module and OS Update PP-Module is not repeated here. See section 3.4.2.4 for complete list of organizational security policies.

4.5 Assumptions

The definition of assumptions from base PP, LPAe PP-Module, IPAe PP-Module and OS Update PP-Module is not repeated here. See section 3.4.2.5 for list of assumptions.

Additionally, the assumption A.Process-Sec-IC is defined as in section 3.4 of [PP-84].

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 base PP, LP Ae PP-Module, IP Ae PP-Module and OS Update PP-module from [PP-eUICC] are not repeated here. See section 3.4.3 for complete list is Security Objectives for the TOE.

The definition of this security objective has been refined as follows since the LUIe is not implemented in the TOE:

- **O.DATA-INTEGRITY-LPAe**
The TOE shall avoid unauthorised modification of the following data when managed or manipulated by the TOE:
 - Keys:
 - D.LPAe_KEYS
 - Management data:
 - D.LPAe_DEVICE_INFO.

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

Sec. Objectives for the TOE	Description
O.IC.PROOF_OF_IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: (1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification). (2) It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PRE, S.PPI, and S.TELECOM). (3) It allows the S.PRE, S.PPI, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection). (4) It provides a means to perform memory operations atomically for S.PRE, S.PPI, and S.TELECOM.
O.IC.RECOVERY	If there is a loss of power while an operation is in progress, the underlying IC must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.

O.RE.PRE-PPI	The Runtime Environment shall provide secure means for card management activities, including: ○ load of a package file, or installation of a package file, ○ extradition of a package file or an application, ○ personalization of an application or a Security Domain, ○ deletion of a package file or an application, ○ privileges update of an application or a Security Domain, ○ 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.

5.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the TOE from base PP, LP Ae PP-Module, IP Ae PP-Module and OS Update PP-module from [PP-eUICC] are not repeated here. See section 3.4.3.2 for list of Security Objectives for the Operational Environment.

Additionally, the OE.Process-Sec-IC is defined as is in Section 4.3 of [PP-84].

5.3 Security Objectives Rationale

5.3.1 Threats

5.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

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

- O.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP+ and MNO OTA Platform) will access the Security Domains functions and content;
- OE.SM-DP+ and OE.MNO protect the corresponding credentials when used 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.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.
- OE.SM-DP+ and OE.EIM (SGP.32) protect the corresponding credentials when used off- card. The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY).

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

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

T.PROFILE-MNG-INTERCEPTION

Commands and profiles are transmitted by the SM-DP+ to its on-card representative (ISD-P), while profile data (including meta-data such as PPRs) is also transmitted by the MNO OTA Platform to its on-card representative (MNO-SD).

Consequently, the TSF ensures:

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

Since the MNO-SD Security Domain is not part of the TOE, the operational environment has to guarantee that it will securely use the SCP80/81 secure channel provided by the TOE (OE.MNO-SD). OE.SM-DP+, OE.MNO and OE.EIM (SGP.32) ensure that the credentials related to the secure channels will not be disclosed when used by off-card actors.

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

5.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

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

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

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

T.IDENTITY-INTERCEPTION

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

OE.CI ensures that the 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-IPAd ensures that the interfaces ES10a, ES10b and ES10c are trusted paths to the LPAd/IPA.

5.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS

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

5.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

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

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

5.3.1.7 LP Ae Threats

T.PLATFORM-MNG-INTERCEPTION-LPDe

The SM-DP+ transmits Profiles (Bound Profile Packages) to the LP Ae (LPDe).

Consequently, the TSF ensures:

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

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

T.PLATFORM-MNG-INTERCEPTION-LDSe

The SM-DS transmits Events to the LP Ae (LDSe).

Consequently, the TSF ensures:

- Security of the transmission to the (O.SECURE-CHANNELS-LP Ae and O.INTERNAL-SECURE-CHANNELS-LP Ae) by requiring authentication from SM-DS, 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-DS ensures that the credentials related to the secure channels will not be disclosed when used by off-card actors.

T.UNAUTHORIZED-PLATFORM-MNG-LP Ae

The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY). In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required:

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

T.PROFILE-MNG-ELIGIBILITY-LP Ae

Device Info, transmitted by the LP Ae to the eUICC for signature, is 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 among the LP Ae and other security domains of the TOE (O.INTERNAL-SECURE-CHANNELS-LP Ae) by protecting the transmission from unauthorized disclosure, modification and replay; These secure channel relies upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

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

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

T.LOGICAL-ATTACK-LP Ae

This threat is covered by controlling the information flow between the LP Ae security domain and the platform layer 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 API of LP Ae shall ensure atomic transactions (O.IC.SUPPORT). Whenever sensitive data of the TOE are processed by LP Ae, confidentiality and integrity must be protected at all times by the Runtime Environment (O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY). However these sensitive data are also be processed by the Platform layer of the TOE, which are not protected by these mechanisms.

Consequently,

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

The following objectives for the operational environment are also required:

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

T.PHYSICAL-ATTACK-LP Ae

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

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

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

Since the TOE cannot only rely on the IC protection measures, the TOE shall enforce any necessary mechanism to ensure resistance against side channels (O.DATA-CONFIDENTIALITY-LP Ae, O.RE.DATA-CONFIDENTIALITY).

5.3.1.8 IP Ae Threats

T.PLATFORM-MNG-INTERCEPTION-IP Ae

The SM-DP+ transmits Profiles (Bound Profile Packages) to the IP Ae, the SM-DS transmits Events to the IP Ae.

Consequently, the TSF ensures:

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

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

T.UNAUTHORIZED-PLATFORM-MNG-IP Ae

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

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

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

T.PROFILE-MNG-ELIGIBILITY-IP Ae

Device Info, transmitted by the IP Ae to the eUICC for signature, is 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 among the IP Ae and other security domains of the TOE (O.INTERNAL-SECURE-CHANNELS-IP Ae) by protecting the transmission from unauthorized disclosure, modification and replay; These secure channel relies upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

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

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

T.LOGICAL-ATTACK-IP Ae

This threat is covered by controlling the information flow between the IP Ae security domain and the platform layer 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 API of IP Ae shall ensure atomic transactions (O.IC.SUPPORT).

Whenever sensitive data of the TOE are processed by IP Ae, confidentiality and integrity must be protected at all times by the Runtime Environment (O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY). However these sensitive data are also be processed by the Platform layer of the TOE, which are not protected by these mechanisms. Consequently,

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

- the Platform layer must protect the confidentiality and integrity of the sensitive data it processes, while applications must use the protection mechanisms provided by the Runtime Environment (O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.DATA-CONFIDENTIALITY-IPaE, O.DATA-INTEGRITY-IPaE).

The following objectives for the operational environment are also required:

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

T.PHYSICAL-ATTACK-IPaE

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

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

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

Since the TOE cannot only rely on the IC protection measures, the TOE shall enforce any necessary mechanism to ensure resistance against side channels (O.DATA-CONFIDENTIALITY-IPaE, O.RE.DATA-CONFIDENTIALITY).

5.3.1.9 OS Update Threats

T.CONFID-UPDATE-IMAGE.LOAD

This threat is countered mainly by confidentiality mechanisms provided by the secure communication of the OS Update mechanism.

O.CONFID-UPDATEIMAGE.LOAD counters the threat by ensuring the confidentiality of D.UPDATE_IMAGE during installing it on the TOE.

OE.CONFID_UPDATE_IMAGE.CREATE counters the threat by ensuring that the D.UPDATE_IMAGE is not transferred in plain and that the keys are kept secret.

T.INTEG-UPDATE-IMAGE.LOAD

This threat is countered mainly by integrity mechanisms provided by the secure communication of the OS Update mechanism.

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

OE.VERIFICATION counters the threat directly by ensuring the authenticity and integrity of D.UPDATE_IMAGE.

T.UNAUTH-UPDATE-IMAGE.LOAD

This threat is countered mainly by authentication mechanisms provided by the secure communication of the OS Update mechanism.

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

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

OE.VERIFICATION counters the threat directly by ensuring the authenticity and integrity of D.UPDATE_IMAGE.

T.INTERRUPT_OSU

This threat is countered mainly by recovery mechanisms provided by OS Update mechanism.

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

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

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

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-IPAd, A.ACTORs, A.ACTORs-LPAe and A.ACTORs-IP Ae are defined as in [PP-eUICC]. The assumptions A.VERIFICATION and A.CAP_FILE are defined as in [PP-JCS]. The assumption A.Process-Sec-IC is defined as in Section 3.4 of [PP-84]. A.APPLICATIONS is directly upheld by OE.CODE-EVIDENCE and OE.APPLICATIONS.

5.3.4 Rationale Tables

5.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PRE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Sec. 5.3.1.1
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, OE.APPLICATIONS, OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.SM-DP+, OE.EIM (SGP.32)	Sec. 5.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD, OE.EIM (SGP.32)	Sec. 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+, O.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Sec. 5.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	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-IPAd	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, 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
T.PLATFORM-MNG-INTERCEPTION-LPDe	O.RE.SECURE-COMM, OE.SM-DP+, O.SECURE-CHANNELS-LPAe, O.INTERNAL-SECURE-CHANNELS-LPAe	Sec. 5.3.1.7
T.PLATFORM-MNG-INTERCEPTION-LDSe	O.RE.SECURE-COMM, OE.SM-DS, O.SECURE-CHANNELS-LPAe, O.INTERNAL-SECURE-CHANNELS-LPAe	Sec. 5.3.1.7
T.UNAUTHORIZED-PLATFORM-MNG-LPAe	OE.APPLICATIONS, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Sec. 5.3.1.7
T.PROFILE-MNG-ELIGIBILITY-LPAe	O.RE.SECURE-COMM, O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-INTEGRITY-LPAe, OE.SM-DP+, O.RE.DATA-INTEGRITY	Sec. 5.3.1.7
T.LOGICAL-ATTACK-LPAe	O.OPERATE, O.API, O.RE.API, O.RE.CODE-EXE, OE.APPLICATIONS, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY, O.DATA-CONFIDENTIALITY	Sec. 5.3.1.7
T.PHYSICAL-ATTACK-LPAe	O.DATA-CONFIDENTIALITY-LPAe, O.IC.SUPPORT, O.IC.RECOVERY, O.RE.DATA-CONFIDENTIALITY	Sec. 5.3.1.7
T.PLATFORM-MNG-INTERCEPTION-IPaE	O.SECURE-CHANNELS-IPaE, O.INTERNAL-SECURE-CHANNELS-IPaE, O.RE.SECURE-COMM, OE.SM-DP+, OE.SM-DS	Sec. 5.3.1.8
T.UNAUTHORIZED-PLATFORM-MNG-IPaE	O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.APPLICATIONS	Sec. 5.3.1.8
T.PROFILE-MNG-ELIGIBILITY-IPaE	O.INTERNAL-SECURE-CHANNELS-IPaE, O.RE.SECURE-COMM, OE.SM-DP+, O.DATA-INTEGRITY-IPaE, O.RE.DATA-INTEGRITY	Sec. 5.3.1.8
T.LOGICAL-ATTACK-IPaE	O.OPERATE, O.API, O.RE.API, O.RE.CODE-EXE, OE.APPLICATIONS, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY, O.DATA-CONFIDENTIALITY	Sec. 5.3.1.8

T.PHYSICAL-ATTACK-IP Ae	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY-IP Ae, O.RE.DATA-CONFIDENTIALITY	Sec. 5.3.1.8
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATEIMAGE.LOAD, OE.CONFID_UPDATE_IMAGE.CREATE	Sec. 5.3.1.9
T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE, OE.VERIFICATION	Sec. 5.3.1.9
T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE, O.AUTH-LOAD-UPDATE-IMAGE, OE.VERIFICATION	Sec. 5.3.1.9
T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE, O.TOE_IDENTIFICATION, O.SECURE_AC_ACTIVATION	Sec. 5.3.1.9

Table 16 Threats and Security Objectives- Coverage

Security Objectives	Threats
O.PRE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK, T.LOGICAL-ATTACK-LPAe, T.LOGICAL-ATTACK-IP Ae
O.API	T.LOGICAL-ATTACK, T.LOGICAL-ATTACK-LPAe, T.LOGICAL-ATTACK-IP Ae
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK, T.LOGICAL-ATTACK-LPAe, T.LOGICAL-ATTACK-IP Ae
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK, T.LOGICAL-ATTACK-LPAe, T.LOGICAL-ATTACK-IP Ae
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DP+	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PROFILE-MNG-ELIGIBILITY-LPAe, T.PLATFORM-MNG-INTERCEPTION-IP Ae, T.PROFILE-MNG-ELIGIBILITY-IP Ae

OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.EIM (SGP.32)	T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION
O.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK, T.LOGICAL-ATTACK-LPaE, T.PHYSICAL-ATTACK-LPaE , T.LOGICAL-ATTACK-IPaE, T.PHYSICAL-ATTACK-IPaE
O.IC.RECOVERY	T.PHYSICAL-ATTACK, T.PHYSICAL-ATTACK-LPaE, T.PHYSICAL-ATTACK-IPaE
O.RE.PRE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PLATFORM-MNG-INTERCEPTION-LDSe, T.PROFILE-MNG-ELIGIBILITY-LPaE, T.PLATFORM-MNG-INTERCEPTION-IPaE, T.PROFILE-MNG-ELIGIBILITY-IPaE
O.RE.API	T.LOGICAL-ATTACK, T.UNAUTHORIZED-PROFILE-MNG, T.LOGICAL-ATTACK-LPaE, T.LOGICAL-ATTACK-IPaE
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK, T.UNAUTHORIZED-PLATFORM-MNG-LPaE, T.LOGICAL-ATTACK-LPaE, T.PHYSICAL-ATTACK-LPaE, T.UNAUTHORIZED-PLATFORM-MNG-IPaE, T.LOGICAL-ATTACK-IPaE, T.PHYSICAL-ATTACK-IPaE
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.UNAUTHORIZED-PLATFORM-MNG-LPaE, T.PROFILE-MNG-ELIGIBILITY-LPaE, T.LOGICAL-ATTACK-LPaE, T.UNAUTHORIZED-PLATFORM-MNG-IPaE, T.PROFILE-MNG-ELIGIBILITY-IPaE, T.LOGICAL-ATTACK-IPaE
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK, T.LOGICAL-ATTACK-LPaE, T.LOGICAL-ATTACK-IPaE
O.SECURE-CHANNELS-LPaE	T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PLATFORM-MNG-INTERCEPTION-LDSe
O.INTERNAL-SECURE-CHANNELS-LPaE	T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PLATFORM-MNG-INTERCEPTION-LDSe, T.PROFILE-MNG-ELIGIBILITY-LPaE
O.DATA-CONFIDENTIALITY-LPaE	T.PHYSICAL-ATTACK-LPaE
O.DATA-INTEGRITY-LPaE	T.PROFILE-MNG-ELIGIBILITY-LPaE,

O.SECURE-CHANNELS-IPaE	T.PLATFORM-MNG-INTERCEPTION-IPaE
O.INTERNAL-SECURE-CHANNELS-IPaE	T.PLATFORM-MNG-INTERCEPTION-IPaE, T.PROFILE-MNG-ELIGIBILITY-IPaE
O.DATA-CONFIDENTIALITY-IPaE	T.PHYSICAL-ATTACK-IPaE
O.DATA-INTEGRITY-IPaE	T.PROFILE-MNG-ELIGIBILITY-IPaE
O.SECURE_LOAD_ACODE	T.INTEG-UPDATE-IMAGE.LOAD, T.UNAUTH- UPDATE-IMAGE.LOAD, T.INTERRUPT_OSU
O.SECURE_AC_ACTIVATION	T.INTERRUPT_OSU
O.TOE_IDENTIFICATION	T.INTERRUPT_OSU
O.CONFID-UPDATEIMAGE.LOAD	T.CONFID-UPDATE-IMAGE.LOAD
O.AUTH-LOAD-UPDATE-IMAGE	T.UNAUTH-UPDATE-IMAGE.LOAD
OE.TRUSTED-PATHS-LPAd-IPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL- ATTACK, T.UNAUTHORIZED-PLATFORM-MNG-LPae, T.LOGICAL-ATTACK-LPae, , T.UNAUTHORIZED- PLATFORM-MNG-IPaE, T.LOGICAL-ATTACK-IPaE
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL- ATTACK
OE.VERIFICATION	T.INTEG-UPDATE-IMAGE.LOAD, T.UNAUTH- UPDATE-IMAGE.LOAD
OE.CAP_FILE	
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG- INTERCEPTION
OE.SM-DS	T.PLATFORM-MNG-INTERCEPTION-LDSe, T.PLATFORM-MNG-INTERCEPTION-IPaE
OE.CONFID_UPDATE_IMAGE.CREATE	T.CONFID-UPDATE-IMAGE.LOAD
OE.Process-Sec-IC	

Table 17 Security Objectives and threats

5.3.4.2 Organizational Security Policies Rationale

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

Table 18 Organizational Security Policies and Security Objectives-Coverage

Security Objectives	Organizational Security Policies
O.PRE-PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE

O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-DP+	
OE.MNO	
OE.EIM (SGP.32)	
O.IC.PROOF_OF_IDENTITY	
O.IC.SUPPORT	
O.IC.RECOVERY	
O.RE.PRE-PPI	OSP.LIFE-CYCLE
O.RE.SECURE-COMM	
O.RE.API	
O.RE.DATA-CONFIDENTIALITY	
O.RE.DATA-INTEGRITY	
O.RE.IDENTITY	
O.RE.CODE-EXE	
O.SECURE-CHANNELS-LPAe	
O.INTERNAL-SECURE-CHANNELS-LPAe	
O.DATA-CONFIDENTIALITY-LPAe	
O.DATA-INTEGRITY-LPAe	
O.SECURE-CHANNELS-IP Ae	
O.INTERNAL-SECURE-CHANNELS-IP Ae	
O.DATA-CONFIDENTIALITY-IP Ae	
O.DATA-INTEGRITY-IP Ae	
O.SECURE_LOAD_ACODE	
O.SECURE_AC_ACTIVATION	
O.TOE_IDENTIFICATION	
O.CONFID-UPDATEIMAGE.LOAD	
O.AUTH-LOAD-UPDATE-IMAGE	
OE.CODE-EVIDENCE	
OE.VERIFICATION	
OE.Process-Sec-IC	

Table 19 Security Objectives and Organizational Security Policies

5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the OE	Rationale
A.TRUSTED-PATHS-LPA _d	OE.TRUSTED-PATHS-LPA _d -IPA _d	Sec. 5.3.3
A.ACTOR _S	OE.CI, OE.SM-DP+, OE.MNO, OE.EIM (SGP.32), OE.SM-DS	Sec. 5.3.3
A.APPLICATION _S	OE.APPLICATION _S , OE.CODE-EVIDENCE	Sec. 5.3.3
A.ACTOR _S -LPA _e	OE.CI, OE.SM-DP+, OE.MNO	Sec. 5.3.3
A.ACTOR _S -IPA _e	OE.SM-DS, OE.SM-DP+, OE.EIM	Sec. 5.3.3
A.CAP_FILE	OE.CAP_FILE	Sec. 5.3.3
A.VERIFICATION	OE.VERIFICATION	Sec. 5.3.3
A.Process-Sec-IC	OE.Process-Sec-IC	Sec. 5.3.3

Table 20 Assumptions and Security Objectives for the Operational Environment-Coverage

Security Objectives for the OE	Assumptions
OE.CI	A.ACTOR _S , A.ACTOR _S -LPA _e
OE.SM-DP+	A.ACTOR _S , A.ACTOR _S -LPA _e , A.ACTOR _S -IPA _e
OE.SM-DS	A.ACTOR _S , A.ACTOR _S -IPA _e
OE.MNO	A.ACTOR _S , A.ACTOR _S -LPA _e
OE.EIM (SGP.32)	A.ACTOR _S , A.ACTOR _S -IPA _e
OE.TRUSTED-PATHS-LPA _d -IPA _d	A.TRUSTED-PATHS-LPA _d -IPA _d
OE.APPLICATION _S	A.APPLICATION _S
OE.CODE-EVIDENCE	A.APPLICATION _S
OE.MNO-SD	
OE.VERIFICATION	A.VERIFICATION
OE.CAP_FILE	A.CAP_FILE
OE.CONFID_UPDATE_IMAGE.CREATE	
OE.Process-Sec-IC	A.Process-Sec-IC

Table 21 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 FAU_SAS – Audit Data Storage

The extended components definition (FAU_SAS.1) from [PP-84] or [PP-117], section 5.3 has been taken with no modification.

7 Security Functional requirements

The following conventions are used in the definitions of the SFRs:

- The assignment operations are marked with **bold** font.
- The selection operations are marked with **bold** and *italic* font.
- Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.
- Refinements, if applicable, have been identified in **bold** font.

Moreover, selections and assignments that have already been made in the different protection profiles ([PP-eUICC], [PP-JCS] and [PP-GP]) are in **bold**, and the original text on which the selection or assignment has been made is not reminded.

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

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

- **SM-DP+ OID is associated to S.ISD-R, acting on behalf of U.SM-DP+;**
- **MNO OID is associated to U.MNO-SD, acting on behalf of U.MNO-OTA;**
- **SM-DS OID is associated to S.ISD-R, acting on behalf of U.SM-DS;**
- **[selection: eIM ID is associated to S.ISD-R, acting on behalf of U.EIM].**

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

- **Initial association of SM-DP+ OID and MNO OID requires U.SM-DP+ to be authenticated**

via "CERT.DPauth.ECDSA" ;

- Initial association of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA" ;
- [selection: Initial association of eIM ID requires U.EIM to be authenticated via CERT.EIM.ECDSA (SGP.32)].

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

- change of SM-DP+ OID requires U.SM-DP+ to be authenticated via "CERT.DPauth.ECDSA" ;
- change of MNO OID is not allowed;
- change of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA" ;
- [selection: change of eIM ID requires U.EIM to be authenticated via "CERT.EIM.ECDSA" (SGP.32)].

FIA_UAU.4/EXT Single-use authentication mechanisms

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

- U.SM-DP+
- U.MNO-OTA
- [selection: U.EIM (SGP.32)]

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow
[assignment:

- application selection
- requesting data that identifies the eUICC]

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/Base User attribute definition

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

- CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-DP+;

- MNO OID belonging to U.MNO-OTA;
- AID belonging to U.MNO-SD;
- CERT.DSauth.ECDSA and SM-DS OID belonging to U.SM-DS;
- [selection: CERT.EIM.ECDSA and eIM ID belonging to U.EIM].

FIA_API.1 Authentication Proof of Identity

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

7.1.2 Communication

FDP_IFC.1/SCP Subset information flow control

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

FDP_IFF.1/SCP Simple security attributes

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

- **users/subjects:**
 - U.SM-DP+ 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-DP+ and S.ISD-R if it is not performed in a SCP-SGP22 secure channel.

FTP_ITC.1/SCP Inter-TSF trusted channel

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

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

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 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-DP+ and U.MNO-OTA
 - Downloaded objects from U.SM-DP+ and U.MNO-OTA
- when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SCP The TSF shall **use [assignment: 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

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

[assignment:

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

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: symmetric keys via PUT KEY, asymmetric keys via STORE DATA]** that meets the following: **[assignment: SGP.22 [SGP.22] and GP [GPCS]]**

FCS_CKM.6/SCP-SM Cryptographic key destruction

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

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

FCS_CKM.6/SCP-MNO Cryptographic key destruction

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

FCS_CKM.6.2/SCP-MNO The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-SM in accordance with a specified cryptographic key destruction method **[assignment: overwriting keys with random values]** 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", and **[selection: no additional attributes]**
- **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
 - in case a currently enabled S.ISD-P has to be disabled, the PPR data of this S.ISD-P allows its disabling, and
 - **[selection: no additional conditions]**.
- **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, S.ECASD
- **objects:** data and attributes of ECASD,
- **operations:**
 - execution of a ECASD function
 - access to output data of these functions,
- [assignment: additional operations defined by the interfaces ES8+ (SM-DP+ – eUICC), and ES10x (LPA – eUICC)

FDP_ACF.1/ECASD Security attribute based access control

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

- **subjects:** S.ISD-R, with security attribute “AID” , S.ECASD
- **objects:** data and attributes of 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.CIECDSA)
 - Creation of an eUICC signature on material provided by an ISD-R.
 - access to output data of these functions.
 - [assignment: O.SECURE-CHANNELS, O.INTERNAL-SECURE-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.DSauth.ECDSA provided by an ISD-R, with the eSIM CA public key (D.PK.CIECDSA)
 - Creation of an 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

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

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

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)"
- Platform code (S.PRE, S.PPI, S.TELECOM)

information:

- D.PROFILE_NAA_PARAMS
- D.PROFILE_RULES
- D.PLATFORM_RAT

operations:

- installation of a profile
- PPR and RAT enforcement
- network authentication.
- *[selection: no additional operations]*

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

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

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

FDP_IFF.1.3/Platform_services [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.PRE, S.PPI or S.TELECOM API specific functions:**
 - **Installation of a profile**
 - **PPR and RAT enforcement**
 - **Network authentication [selection: no additional functions]**
- **[assignment: none].**

7.1.5 Security management

FCS_RNG.1 Random number generation

Refinement:

FCS_RNG.1.1 The TSF shall provide a **[selection: physical]** random number generator **Class PTG.2 according to [AIS31]** that implements: **[assignment:**

- **PTG.2.1 A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.**
- **PTG.2.2 If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.**
- **PTG.2.3 The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.**
- **PTG.2.4 The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.**
- **PTG.2.5 The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time].**

FCS_RNG.1.2 The TSF shall provide **[selection: assignment: [32-bit numbers]]** that meet **[assignment:**

- **PTG.2.6 Test procedure A, as defined in [AIS31] does not distinguish the internal random numbers from output sequences of an ideal RNG.**
- **PTG.2.7 The average Shannon entropy per internal random bit exceeds 0.997].**

FPT_EMS.1/Base TOE Emanation

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

ID	Emission	Attack surface	TSF data	User data
1	[assignment: variations in power consumption or timing during command execution]	Any	-	- o D.SECRETS; - o D.SK.EUICC.ECDSA and the secret keys which are part of the following keysets: - o D.MNO_KEYS, - o D.PROFILE_NAA_PARAMS.

FDP_SDI.1/Base Stored data integrity monitoring

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

FDP_RIP.1/Base Subset residual information protection

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

FPT_FLS.1/Base Failure with preservation of secure state

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

FMT_MSA.1/PLATFORM_DATA Management of security attributes

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

FMT_MSA.1/RULES Management of security attributes

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

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

FMT_MSA.1/CERT_KEYS Management of security attributes

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

- o D.CERT.EUICC.ECDSA
- o D.PK.CIECDSA
- o D.CERT.EUM.ECDSA
- o D.MNO_KEYS

to

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

FMT_SMF.1/Base Specification of Management Functions

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

FMT_SMR.1/Base Security roles

FMT_SMR.1.1/Base The TSF shall maintain the roles

- External users:
 - U.SM-DP+
 - U.MNO-SD
 - U.MNO-OTA
 - U.SM-DS
 - [*selection: U.EIM (SGP.32)*]
- Subjects:
 - S.ISD-R
 - S.ISD-P
 - S.EC ASD
 - S.PPI
 - S.PRE
 - S.TELECOM.

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

FMT_MSA.1/RAT Management of security attributes

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

FMT_MSA.3/Base Static attribute initialization

The definition of this SFR is present in [PP-eUICC] as FMT_MSA.3/Base and it is unchanged within this ST.
The iteration /Base is added.

7.1.6 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

Refinement:

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.
- [selection: no additional standards].

FCS_CKM.2/Mobile_network Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: **Network Authentication keys as part of the D.PROFILE_NAA_PARAMS loaded during profile installation**] that meets the following: [assignment: SGP.22].

FCS_CKM.6/Mobile_network Cryptographic key destruction

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

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

7.2 LP Ae Security Functional Requirements

The introduction and security attributes are leveraged from [PP-eUICC] section 7.7.1.1.

7.2.1 Identification and authentication

FIA_UID.1/LP Ae Timing of identification

FIA_UID.1.1/LP Ae The TSF shall allow

- application selection
- requesting data that identifies the eUICC
- [assignment: and no other actions].

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

FIA_UID.1.2/LP Ae 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/LP Ae Timing of authentication

FIA_UAU.1.1/LP Ae The TSF shall allow

- application selection
- requesting data that identifies the eUICC
- user identification
- [assignment: and no other actions]

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

FIA_UAU.1.2/LP Ae 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/LP Ae User-subject binding

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

FIA_UAU.4/LP Ae Single-use authentication mechanisms

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

FIA_ATD.1/LP Ae User attribute definition

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

7.2.2 Communication

FDP_IFC.1/LP Ae Subset information flow control

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

FDP_IFF.1/LP Ae Simple security attributes

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

- **users/subjects:**
 - **U.SM-DP+ and S.LP Ae, with security attribute D.LP Ae_KEYS**
 - **U.SM-DS and S.LP Ae, with security attribute D.LP Ae_KEYS**
- **information: transmission of commands.**

FDP_IFF.1.2/LP Ae The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment: none]**.

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

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

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

- **The TOE shall reject communication between U.SM-DP+ and S.LP Ae if it is not performed in a TLS secure channel;**
- **The TOE shall reject communication between U.SM-DS and S.LP Ae if it is not performed in a TLS secure channel.**

FTP_ITC.1/LP Ae Inter-TSF trusted channel

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

FDP_ITC.1.3/LP Ae The TSF shall initiate communication via the trusted channel for **[assignment:**

- The TSF shall permit the LP Ae to open a TLS secure channel to SM-DP+ and transmit the following operations:
 - ES9+.InitiateAuthentication
 - ES9+.GetBoundProfilePackage
 - ES9+.AuthenticateClient
 - ES9+.HandeNotification
 - ES9+.CancelSession
- The TSF shall permit the LP Ae to open a TLS secure channel to SM-DS and transmit the following operations:
 - ES11.InitiateAuthentication
 - ES11.AuthenticateClient

].

FDP_ITC.2/LP Ae Import of user data with security attributes

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

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

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

FPT_TDC.1/LP Ae Inter-TSF basic TSF data consistency

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

- Commands from U.SM-DP+ and U.SM-DS
- Downloaded objects from U.SM-DP+

when shared between the TSF and another trusted IT product.

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

FDP_UCT.1/LP Ae Basic data exchange confidentiality

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

FDP_UIT.1/LP Ae Data exchange integrity

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

FCS_CKM.1/LP Ae Cryptographic key generation

FCS_CKM.1.1/LP Ae The TSF shall generate cryptographic keys in accordance with a specified

cryptographic key generation algorithm **Elliptic Curves Key Agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following: [assignment:

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

FCS_CKM.6/LPAe Cryptographic key destruction

FCS_CKM.6.1/LPAe The TSF shall destroy **D.LPAe_KEYS** when [selection: *no longer needed*].

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

7.2.3 Security management

FPT_EMS.1/LPAe TOE Emanation

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

ID	Emission	Attack surface	TSF data	User data
1	[assignment: variations in power consumption or timing during command execution]	Any	D.LPAe_KEYS	[assignment: the secret keys which are part of the following keysets: • D.MNO_KEYS, • D.PROFILE_NAA_PARAMS.]

FDP_SDI.1/LPAe Stored data integrity monitoring

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

Note: The notion of integrity-sensitive data covers the following assets that require to be protected against unauthorized modification:

- Management data:
 - **D.LPAe_DEVICE_INFO**
- Keys:
 - **D.LPAe_KEYS**

FDP_RIP.1/LPAe Subset residual information protection

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

FMT_SMF.1/LPAe Specification of Management Functions

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

FMT_SMR.1/LP Ae Security roles

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

7.3 IP Ae Security Functional Requirements

7.3.1 Identification and authentication

FIA_UID.1/IP Ae Timing of identification

FIA_UID.1.1/IP Ae The TSF shall allow

- application selection
- requesting data that identifies the eUICC
- [assignment: and no other actions].

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

FIA_UID.1.2/IP Ae 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/IP Ae Timing of authentication

FIA_UAU.1.1/IP Ae The TSF shall allow

- application selection
- requesting data that identifies the eUICC
- user identification
- [assignment: and no other actions]

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

FIA_UAU.1.2/IP Ae 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/IP Ae User-subject binding

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

FIA_UAU.4/IP Ae Single-use authentication mechanisms

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

FIA_ATD.1/IP Ae User attribute definition

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

7.3.2 Communication

FDP_IFC.1/IP Ae Subset information flow control

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

FDP_IFF.1/IP Ae Simple security attributes

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

- **users/subjects:**
 - **U.SM-DP+ and S.IP Ae, with security attribute D.IP Ae_KEYS**
 - **U.SM-DS and S.IP Ae, with security attribute D.IP Ae_KEYS**
 - **U.EIM and S.IP Ae, with security attribute D.IP Ae_KEYS**
- **information: transmission of commands.**

FDP_IFF.1.2/IP Ae The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment: none]**.

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

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

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

- **The TOE shall reject communication between U.SM-DP+ and S.IP Ae if it is not performed in a TLS secure channel;**
- **The TOE shall reject communication between U.SM-DS and S.IP Ae if it is not performed in a TLS secure channel.**
- **The TOE shall reject communication between U.EIM and S.IP Ae if it is not performed in a TLS/DTLS (or equivalent) secure channel.**

FTP_ITC.1/IP Ae Inter-TSF trusted channel

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

FTP_ITC.1.3/IP Ae The TSF shall initiate communication via the trusted channel for [assignment: the following cases:

- The TSF shall permit the IP Ae to open a TLS secure channel to SM-DP+ and transmit the following operations:
 - ES9+.InitiateAuthentication
 - ES9+.GetBoundProfilePackage
 - ES9+.AuthenticateClient
 - ES9+.HandleNotification
 - ES9+.CancelSession
 - ES9+-.ConfirmDeviceChange
- The TSF shall permit the IP Ae to open a TLS secure channel to SM-DS and transmit the following operations:
 - ES11.InitiateAuthentication
 - ES11.AuthenticateClient
 - ES11.CheckEvent
- The TSF shall permit the IP Ae to open a TLS/DTLS secure channel to eIM and transmit the following operations:
 - ESipa.InitiateAuthentication
 - ESipa.GetBoundProfilePackage
 - ESipa.AuthenticateClient
 - ESipa.HandleNotification
 - ESipa.CancelSession
 - ESipa.GetEimPackage
 - ESipa.TransferEimPackage
 - ESipa.ProvideEimPackageResult

].

FDP_ITC.2/IP Ae Import of user data with security attributes

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

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

FDP_ITC.2.3/IP Ae 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/IP Ae 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/IP Ae The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: no additional importation control rules]**.

FPT_TDC.1/IP Ae Inter-TSF basic TSF data consistency

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

- **Commands from U.SM-DP+, U.EIM and U.SM-DS**
- **Downloaded objects from U.SM-DP+ and U.EIM**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/IP Ae The TSF shall use **[assignment: no additional interpretation rules]** when interpreting the TSF data from another trusted IT product.

FDP_UCT.1/IP Ae Basic data exchange confidentiality

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

FDP_UIT.1/IP Ae Data exchange integrity

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

FCS_CKM.1/IP Ae Cryptographic key generation

FCS_CKM.1.1/IP Ae The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curve Key Agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following **[assignment:**

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

].

FCS_CKM.6/IP Ae Cryptographic key destruction

FCS_CKM.6.1/IP Ae The TSF shall destroy **D.IP Ae_KEYS** when **[selection: no longer needed]**.

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

7.3.3 Security management

FPT_EMS.1/IP Ae TOE Emanation

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

ID	Emission	Attack surface	TSF data	User data
1	[assignment: variations in power consumption or timing during command execution]	Any	D.IP Ae_KEYS	[assignment: the secret keys which are part of the following keysets: • D.MNO_KEYS, • D.PROFILE_NAA_PARAMS.]

FDP_SDI.1/IP Ae Stored data integrity monitoring

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

FDP_RIP.1/IP Ae Subset residual information protection

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

FMT_SMF.1/IP Ae Specification of Management Functions

FMT_SMF.1.1/IP Ae The TSF shall be capable of performing the following management functions: [assignment: Profile State Management functions specified in GSMA SGP.32].

FMT_SMR.1/IP Ae Security roles

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

7.4 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.

7.4.1 CoreLG Security Functional requirements

7.4.1.1 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] and it is unchanged within this ST.

FMT_SMR.1/JC Security roles

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

7.4.1.2 Application Programming Interface

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: see Table 22] and specified cryptographic key sizes [assignment: see Table 22] that meet the following: [assignment: see Table 22].

Iteration	Algorithm	Key sizes	List of standards
/ECDH	ECDH	256 bits	NIST SP 800-56
/SIG_ECC	ECDSA	256 bits	NIST P-256 (FIPS PUB 186-4 Digital Signature Standard) brainpoolP256r1 (BSI TR-03111), Version 1.11 RFC 5639) FRP256V1 (ANSSI ECC FRP256V1)
/TDES	Triple DES	112, 168 bits	SP800-67
/AES	AES	128, 192, 256 bits	FIPS 197

Table 22 Cryptographic keys

FCS_CKM.6/RE Cryptographic key destruction

FCS_CKM.6.1/RE The TSF shall destroy [assignment: Keys listed in Table 22] when [selection: no longer needed].

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

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: the cryptographic operations in Table 23 Cryptographic mechanisms Table 23] in accordance with a specified cryptographic algorithm [assignment: in Table 23 Cryptographic mechanismsTable 23] and cryptographic key sizes [assignment: in Table 23 Cryptographic mechanismsTable 23] that meet the following [assignment: list of standards in Table 23 Cryptographic mechanisms Table 23].

Iteration	Operation	Algorithm	Key sizes	List of standards
/ECDH	Key Agreement	ECDH	256 bits	NIST SP 800-56
/MD	Message digest - hashing	SHA-256	n/a	FIPS 180-4
/MAC_TDES	MAC generation and verification	Triple DES CBC MAC	112, 168 bits	FIPS 46-3 ISO 9797-1
/MAC_AES	MAC generation and verification	AES CBC MAC	128, 192, 256 bits	FIPS 197 ISO 9797-1 SP800-38b
/SIG_ECC	Digital signature generation and verification	ECDSA	256 bits	NIST P-256 (FIPS PUB 186-4 Digital Signature Standard) brainpoolP256r1 (BSI TR-03111), Version 1.11 RFC 5639) FRP256V1 (ANSSI ECC FRP256V1)
/CIPH_TDES_CBC	Encryption and decryption	Triple DES CBC	112, 168 bits	SP800-67
/CIPH_AES_GCM	Encryption and decryption	AES_GCM	128, 192, 256 bits	FIPS 197
/CIPH_AES_CBC	Encryption and decryption	AES_CBC	128, 192, 256 bits	FIPS 197
/HMAC	Signature	HMAC	64 – 1016 bits Based on SHA-256	FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)

Table 23 Cryptographic mechanisms

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.

7.4.1.3 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,
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow
- **[assignment: no additional events].**

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_FLS.1/JC Failure with preservation of secure state

The definition of this SFR is present in [PP-JCS] as FPT_FLS.1 and it is unchanged within this ST. In this ST the iteration /JC is added.

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

FPT_TDC.1.1/JC 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/JC The TSF shall use

- **the rules defined in [JCVM3] specification,**
 - **the API tokens defined in the export files of reference implementation,**
 - **[assignment: and no additional rules]**
- when interpreting the TSF data from another trusted IT product.

7.4.1.4 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: **CAP file 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 an unique CAP file 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 CAP file 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.

7.4.2 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.

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.

7.4.3 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.

7.4.4 RMIG Security Functional Requirements

The TOE does not support RMI features.

7.4.5 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.

7.4.6 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 CAP files** 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 CAP file**, of 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 **CAP FILE LOADING information flow control SFP** based on the following types of subject and information security attributes: **[assignment:**

Subjects:

- S.SD receiving the Card Content Management commands (through APDUs or APIs).
- S.CAD the off-card entity that communicates with the S.SD.

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 behaviour 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 authorise 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 CAP file.
- **[assignment: When none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold].**

FDP_UT.1/CM Data exchange integrity

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

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

FIA_UID.1/CM Timing of identification

FIA_UID.1.1/CM 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/CM 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 **CAP file LOADING information flow control SFP** to restrict the ability to *[selection: modify]* the security attributes **[assignment:**

[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:

- application locking and unlocking (Section 9.6.2 of [GPCS])
- card status interrogation (Section 9.6.6 of [GPCS])
- application status interrogation (Section 9.6.5 of [GPCS])

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.

7.4.7 Card Content Management Security Functional requirements

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when [*selection: [assignment: 1]*] unsuccessful authentication attempts occur related to **the authentication of the origin of a card management operation command**.

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

FIA_UAU.1/GP Timing of authentication

Refinement:

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

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

FDP_UT.1/GP Basic data exchange integrity

FDP_UT.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_UT.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.

FMT_SMR.1.1/GP Security roles

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

7.5 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 and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software*] in the [*assignment: access protected and not changeable areas of the non-volatile memory*].

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.

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.

7.6 OS Update Functional Requirements

The introduction and security attributes definition are present in [PP-GP] section 18.4 and are not repeated here.

7.6.1 OS Update

FDP_ACC.1/OS-UPDATE Subset access control

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

- **Subjects:** S.OS-DEVELOPER is the representative of the OS Developer within the TOE, being responsible for signature verification and decryption of the additional code, before:
 - **Loading**
 - **Installation**
 - **Activation**
 - **[assignment: none]**
 is authorised.
- **Objects:** additional code and associated cryptographic signature
- **Operations:** loading, installation, and activation of additional code.

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

FDP_ACF.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to objects based on the following:

- **Security Attributes:**
 - **The additional code cryptographic signature verification status**
 - **The Identification Data verification status (between the Initial TOE and the additional code).**

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

- The verification of the additional code cryptographic signature (using D.OS-UPDATE_SGNVER-KEY) by S.OS-DEVELOPER is successful.
- The decryption of the additional code prior installation (using D.OS-UPDATE_DEC-KEY) by S.OS-DEVELOPER is successful.
- The comparison between the identification data of both the Initial TOE and the additional code demonstrates that the OS Update operation can be performed.
- [assignment: none].

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

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

FIA_ATD.1/OS-UPDATE User attribute definition

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

FMT_MSA.3/OS-UPDATE Security attribute initialization

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

FMT_SMR.1/OS-UPDATE Security roles

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

FMT_SMF.1/OS-UPDATE Specification of Management Functions

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

FTP_TRP.1/OS-UPDATE Trusted Path

FTP_TRP.1.1/OS-UPDATE The TSF shall provide a communication path between itself and remote that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: disclosure].

FTP_TRP.1.2/OS-UPDATE The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/OS-UPDATE The TSF shall require the use of the trusted path for **the transfer of the additional code to the TOE**.

FCS_COP.1/OS-UPDATE-DEC Cryptographic operation

FCS_COP.1.1/OS-UPDATE-DEC The TSF shall perform **Decryption of the additional code prior installation** in accordance with a specified cryptographic algorithm [assignment: AES decryption in CBC mode] and cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: FIPS 197].

FCS_COP.1/OS-UPDATE-VER Cryptographic operation

FCS_COP.1.1/OS-UPDATE-VER The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm [assignment: AES MAC in CBC mode] and cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: FIPS 197, ISO9797].

FPT_FLS.1/OS-UPDATE Failure with preservation of secure state

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

7.7 Security Functional Requirements Rationale

7.7.1 SFRs for eUICC rationale

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

7.7.2 SFRs for LP Ae rationale

The security functional requirements rationale is the same than the one present in LP Ae module section 7.7.3 from [PP-eUICC].

7.7.3 SFRs for IP Ae rationale

The security functional requirements rationale is the same than the one present in IP Ae module section 9.7.3 from [PP-eUICC].

7.7.4 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.

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

Table 24 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.

Moreover, the objective for the operational environment OE.CARD-MANAGEMENT from [PP-JCS] is converted to objectives for the TOE O.* in current Security Target.

The SFRs rationale is extracted from [PP-JCS].

7.7.5 SFRs for OS Update rationale

The next table shows the objectives related to [PP-eUICC] OS Update module and it' s mapped to Security Functional Requirements extracted from [PP-GP].

Security Objectives	SFR	Rationale
O.SECURE_LOAD_ACODE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-VER, FPT_FLS.1/OS-UPDATE	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code. FCS_COP.1/OS-UPDATE-VER specifies the cryptographic algorithms used to perform digital signature verification of the additional code to be loaded. FPT_FLS.1/OS-UPDATE ensures that the operation is performed in an atomic manner maintaining the integrity of the Additional Code.
O.SECURE_AC_ACTIVATION	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FPT_FLS.1/OS-UPDATE	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code. FPT_FLS.1/OS-UPDATE ensures that the operation is performed in an atomic manner maintaining the integrity of the Activation of the Additional Code.
O.TOE_IDENTIFICATION	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FIA_ATD.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE,	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FIA_ATD.1/OS-UPDATE maintains the additional code ID for each activated additional code.

	FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE	FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code.
O.CONFID-UPDATEIMAGE.LOAD	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code. FTP_TRP.1/OS-UPDATE provides a trusted path during the transmission of the additional code to the TOE for loading. FCS_COP.1/OS-UPDATE-DEC specifies the cryptographic algorithms used to decrypt the additional code prior to installation.
O.AUTH-LOAD-UPDATE-IMAGE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FIA_ATD.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code. FIA_ATD.1/OS-UPDATE maintains the additional code ID for each activated additional code. FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code. FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation. FMT_SMF.1/OS-UPDATE manages the activation of additional code.

Table 25 Security Functional Requirements for OS Update 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.

7.7.6 SFRs for Underlying platform IC rationale

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

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

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

7.8 Security Functional Requirements Dependencies

7.8.1 Dependencies for eUICC SFRs

The security functional requirements dependencies are the same than the ones present in section 6.3.3.1 from [PP-eUICC].

7.8.2 Dependencies for LP Ae SFRs

The security functional requirements dependencies are the same than the ones present in section 7.7.3.3.1 from [PP-eUICC].

7.8.3 Dependencies for IP Ae SFRs

The security functional requirements dependencies are the same than the ones present in section 9.7.3.4.1 from [PP-eUICC].

7.8.4 Dependencies for Runtime Environment SFRs

The security functional requirements dependencies are the same than the ones present in section 7.4.3.1 from [PP-JCS].

For SFRs from [PP-GP], the dependencies are the same to those described in section 7.3.3 of [PP-GP].

Additionally, the dependencies of the iterations added regarding cryptographic mechanisms are listed in the table below:

SFR	Dependency	Iteration	Satisfied Dependencies
FCS_COP.1	(FCS_CKM.1 or FCS_CKM.5 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6).	/ECDH	FCS_CKM.1/ECDH FCS_CKM.6/RE FDP_ITC.2
		/MD	FCS_CKM.6/RE FDP_ITC.2/Installer
		/MAC_TDES	FCS_CKM.1/TDES FCS_CKM.6/RE
		/MAC_AES	FCS_CKM.1/AES FCS_CKM.6/RE
		/SIG_ECC	FCS_CKM.1/SIG_ECC

			FCS_CKM.6/RE
		/CIPH_TDES_CBC	FCS_CKM.1/TDES FCS_CKM.6/RE
		/CIPH_AES_GCM	FCS_CKM.1/AES FCS_CKM.6/RE
		/CIPH_AES_CBC	FCS_CKM.1/AES FCS_CKM.6/RE
		/HMAC	FCS_CKM.1/SCP-SM FCS_CKM.6/RE
FCS_CKM.1	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	/ECDH	FCS_COP.1/ECDH FCS_RNG.1 FCS_CKM.6/RE
		/SIG_ECC	FCS_COP.1/SIG_ECC FCS_RNG.1 FCS_CKM.6/RE
		/TDES	FCS_COP.1/CIPH_TDES* FCS_COP.1/MAC_TDES FCS_RNG.1 FCS_CKM.6/RE
		/AES	FCS_COP.1/CIPH_AES* FCS_COP.1/MAC_AES FCS_RNG.1 FCS_CKM.6/RE
FCS_CKM.6	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5)	/RE	FDP_ITC.2/SCP FDP_ITC.2/Installer

Table 26 Dependencies for Cryptographic Iterations

7.8.5 Dependencies for OS Update SFRs

The security functional requirements dependencies are the same than the ones present in section 18.6 from [PP-GP].

7.8.6 Dependencies for Underlying platform IC SFRs

The dependencies for the SFRs of the underlying platform IC are the following:

SFR	Dependency	Satisfied Dependencies
FAU_SAS.1	No dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	Operational user Guidance

FPT_RCV.4/OS	No dependencies	
--------------	-----------------	--

Table 27 SFRs dependencies for underlying platform IC

8 Statement of Compatibility

This section demonstrates the consistency between the ST TOE and the certified IC platform.

8.1 IC reference

The TOE is mounted on the platform IFX_CCI_00007Ah A11/R11/M11, see [IC_CERT_REPORT] and the ST [IC_ST]. The platform is compliant to [PP-84] and identified with Cert-ID: BSI-DSZ-CC-1272-2026.

The TOE claims evaluation assurance level EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

The platform claims evaluation assurance level EAL6 augmented with ALC_FLR.1 and ATE_SDP.1.

8.2 Security Objectives Consistency

IC Security Objectives	Description	TOE
O.Phys-Manipulation	Protection against Physical Manipulation	This objective is covered by TOE evaluation.
O.Phys-Probing	Protection against Physical Probing	This objective is covered by TOE evaluation.
O.Malfunction	Protection against Malfunction	This objective is covered by TOE evaluation.
O.Leak-Inherent	Protection against Inherent Information Leakage	This objective is covered by TOE evaluation.
O.Leak-Forced	Protection against Forced Information Leakage	This objective is covered by IC evaluation.
O.Abuse-Func	Protection against Abuse of Functionality	This objective is covered by TOE evaluation.
O.Identification	TOE Identification	This objective is covered by TOE evaluation.
O.RND	Random Numbers	This objective is covered by TOE evaluation.
O.Cap_Avail_Loader	Capability and availability of the Loader	This objective is covered by IC evaluation.
O.Ctrl_Auth_Loader	Access control and authenticity for the Loader	This objective is covered by IC evaluation.

IC Security Objectives	Description	TOE
O.Authentication	Authentication to external entities	This objective is covered by TOE evaluation.
O.TDES	Cryptographic service Triple-DES	This objective is covered by TOE evaluation.
O.AES	Cryptographic service AES	This objective is covered by TOE evaluation.
O.Secure_UC_Load	Secure loading of the Update Code	This objective is covered by TOE evaluation.
O.Secure_UC_Activation	Secure activation of the Update Code	This objective is covered by TOE evaluation.
O.FIREWALL	Firewall based Access Control	This objective is covered by TOE evaluation.
O.FFC	Finite Field cryptographic services	This objective is covered by the IC evaluation.
O.RSA	RSA cryptographic services	This objective is covered by the IC evaluation.
O.ECC	Elliptic Curve cryptographic services	This objective is covered by TOE evaluation.
O.ML	Module Lattice cryptographic services	This objective is covered by IC evaluation.
O.HMAC	HMAC Cryptographic services	This objective is covered by TOE evaluation.
O.Hash	Cryptographic service hash	This objective is covered by TOE evaluation.
O.Prot_TSF_Confidentiality	Protection of confidentiality of TSF	This objective is covered by TOE evaluation.

Table 28 IC Security Objectives Consistency

8.3 Security Objectives for the Environment Consistency

IC Security Objectives	Description	TOE
OE.Resp-Appl	Treatment of User Data	This objective is covered by TOE evaluation.
OE.Process-Sec-IC	Protection during composite product manufacturing	This objective is covered by TOE evaluation.
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	This objective is covered by IC evaluation.
OE.Loader_Usage	Secure communication and usage of the Loader	This objective is covered by IC evaluation.
OE.TOE_Auth	External entities authenticating of the TOE	This objective is covered by TOE evaluation.
OE.Secure_UC_Load	User software is required to support secure image loading in phase 7 by providing the relevant key material for the image.	This objective is covered by TOE evaluation.
OE.Secure_Delivery	When the TOE is ordered with a disabled Flash Loader or with an enabled Flash Loader but Mutual Authentication disabled, it does not provide transport protection. Therefore, technical and / or organizational security procedures (e.g. a custom mutual authentication mechanism or a security transport) should be put in place by the customer to secure the personalized TOE during delivery as required by the security needs of the loaded IC Embedded Software.	This objective is covered by the IC evaluation.

Table 29 Security Objectives for the Environment Consistency

8.4 Security Functional Requirements Consistency

The list of the base component-SFRs is separated in three groups:

- **IP_SFR:** Irrelevant base component-SFRs not being used by the composite-ST;
- **RP_SFR-SERV:** Relevant base component-SFRs being used by the composite-ST to implement a security service with associated TSFI;
- **RP_SFR-MECH:** Relevant base component-SFRs being used by the composite-ST because of their security properties providing protection against attacks to the TOE as a whole and being addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the IC.

IC Security Functional Requirements		TOE
FRU_FLT.2	Limited fault tolerance	RP_SFR-MECH
FPT_FLS.1	Failure with preservation of secure state	RP_SFR-MECH
FMT_LIM.1	Limited capabilities	RP_SFR-MECH

IC Security Functional Requirements		TOE
FMT_LIM.2	Limited availability	RP_SFR-MECH
FAU_SAS.1	Audit storage	RP_SFR-SERV
FDP_SDC.1	Stored data confidentiality	RP_SFR-MECH
FDP_SDI.2	Stored data integrity monitoring and action	RP_SFR-MECH
FPT_PHP.3	Resistance to physical attack	RP_SFR-MECH
FPT_SDP.1	Self-secured digital protection	RP_SFR-SERV
FDP_ITT.1	Basic internal transfer protection	RP_SFR-SERV
FPT_ITT.1	Basic internal TSF data transfer protection	RP_SFR-SERV
FDP_IFC.1	Subset information flow control	RP_SFR-SERV
FDP_ITT.1/SDP	Basic internal transfer protection	RP_SFR-SERV
FPT_ITT.1/SDP	Basic internal TSF data transfer protection	RP_SFR-SERV
FDP_IFC.1/SDP	Subset information flow control	RP_SFR-SERV
FCS_RNG.1/TRNG	Random number generation	RP_SFR-SERV
FCS_COP.1/AES	Cryptographic operation - AES	IP_SFR
FCS_CKM.6/AES	Cryptographic key destruction	IP_SFR
FMT_LIM.1/Loader	Limited Capabilities – Loader	RP_SFR-MECH
FMT_LIM.2/Loader	Limited availability – Loader	RP_SFR-MECH
FTP_ITC.1	Inter-TSF trusted channel	RP_SFR-SERV
FDP_UCT.1	Basic data exchange confidentiality	RP_SFR-SERV
FDP_UIT.1	Data exchange integrity	RP_SFR-SERV
FDP_ACC.1/Loader	Subset access control – Loader	RP_SFR-MECH
FDP_ACF.1/Loader	Security attribute-based access control – Loader	RP_SFR-MECH
FMT_MTD.1/Loader	Management of TSF data	RP_SFR-MECH
FMT_SMR.1/Loader	Security roles	RP_SFR-MECH
FMT_SMF.1/Loader	Specification of Management Functions	RP_SFR-MECH
FIA_UID.2/Loader	User identification before any action	RP_SFR-MECH
FPT_FLS.1/Loader	Failure with preservation of secure state	RP_SFR-MECH
FIA_API.1	Authentication Proof of Identity	RP_SFR-SERV
FPT_TST.1	TSF testing	RP_SFR-SERV
FDP_ACC.2/AF	Complete access control	RP_SFR-SERV
FDP_ACF.1/AF	Security attribute-based access control	RP_SFR-SERV

IC Security Functional Requirements		TOE
FMT_MSA.3/AF	Static attribute initialisation	RP_SFR-SERV
FMT_MSA.1/AF/S	Management of security attributes	RP_SFR-SERV
FMT_MSA.1/AF/NS	Management of security attributes	RP_SFR-SERV
FMT_SMF.1/AF	Specification of management functions	RP_SFR-SERV
FMT_SMR.1/AF	Security roles	RP_SFR-SERV
FCS_COP.1/CS/AES/ENC	Cryptographic operation	RP_SFR-SERV
FCS_COP.1/CS/AES/CMAC	Cryptographic operation	IP_SFR
FCS_COP.1/CS/AES/CBC-MAC	Cryptographic operation	RP_SFR-SERV
FCS_COP.1/CS/AES/CCM	Cryptographic operation	IP_SFR
FCS_COP.1/CS/AES/GCM	Cryptographic operation	RP_SFR-SERV
FCS_CKM.6/CS/AES	Timing and event of cryptographic key destruction	IP_SFR
FCS_COP.1/CS/TDES/ENC	Cryptographic operation	RP_SFR-SERV
FCS_COP.1/CS/TDES/RMAC	Cryptographic operation	IP_SFR
FCS_COP.1/CS/TDES/CBC-MAC	Cryptographic operation	RP_SFR-SERV
FCS_CKM.6/CS/TDES	Timing and event of cryptographic key destruction	IP_SFR
FCS_COP.1/CS/HMAC/SHA	Cryptographic operation	IP_SFR
FCS_COP.1/CS/FFC/DH	Cryptographic operation	IP_SFR
FCS_CKM.1/CS/FFC	Cryptographic key operation	IP_SFR
FCS_COP.1/CS/RSA/ENC	Cryptographic operation	IP_SFR
FCS_COP.1/CS/RSA/DEC	Cryptographic operation	IP_SFR
FCS_COP.1/CS/RSA/DEC_CRT	Cryptographic operation	IP_SFR
FCS_COP.1/CS/RSA/SIG	Cryptographic operation	IP_SFR
FCS_COP.1/CS/RSA/SIG_CRT	Cryptographic operation	IP_SFR
FCS_COP.1/CS/RSA/VER	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/ECDSA_SIG	Cryptographic operation	RP_SFR-SERV
FCS_COP.1/CS/ECC/ECDSA_VER	Cryptographic operation	RP_SFR-SERV
FCS_COP.1/CS/ECC/ECDH	Cryptographic operation	RP_SFR-SERV
FCS_COP.1/CS/ECC/PACE_IM	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/X25519	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/X448	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/ECSDSA_SIG	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/ECSDSA_VER	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/EdDSA_SIG	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/EdDSA_VER	Cryptographic operation	IP_SFR

IC Security Functional Requirements		TOE
FCS_COP.1/CS/ECC/HashEdDSA_SIG	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ECC/HashEdDSA_VER	Cryptographic operation	IP_SFR
FCS_CKM.1/CS/ECC/ECDSA	Cryptographic key operation	RP_SFR-SERV
FCS_CKM.1/CS/ECC/EDDSA	Cryptographic key operation	IP_SFR
FCS_CKM.1/CS/ECC/ECDSA	Cryptographic key operation	IP_SFR
FCS_COP.1/CS/ML/ENC	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ML/DEC	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ML/SIG	Cryptographic operation	IP_SFR
FCS_COP.1/CS/ML/VER	Cryptographic operation	IP_SFR
FCS_CKM.1/CS/ML/KEM_GEN	Cryptographic key operation	IP_SFR
FCS_CKM.1/CS/ML/DSA_GEN	Cryptographic key operation	IP_SFR
FCS_COP.1/CS/Hash/SHA1	Cryptographic operation	IP_SFR
FCS_COP.1/CS/Hash/SHA2	Cryptographic operation	IP_SFR
FCS_COP.1/CS/Hash/SHA3	Cryptographic operation	IP_SFR
FCS_COP.1/CS/Hash/XOF	Cryptographic operation	IP_SFR
FCS_RNG.1/CS/PTG2	Random Number Generation	IP_SFR
FCS_RNG.1/CS/PTG3	Random Number Generation	IP_SFR
FCS_RNG.1/CS/DRG3	Random Number Generation	IP_SFR
FCS_RNG.1/CS/DRG4	Random Number Generation	IP_SFR

Table 30 IC Security Functional Requirements Consistency

9 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.

9.1 eUICC security functions

Security Functions (SF)	Description
SF.EUICC.CRYPTO	The TOE implements RSP features as described in [SGP.22]. 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:

Security Functions (SF)	Description
	- 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, PPI, PRE and TELECOM.
SF.EUICC.SCP	The TOE implements RSP features as described in [SGP.22]. Part of these features are supported for additional secure protocol channels which are part of the services provided by the TOE. The SCP in scope are: - ES6 - ES10b - ES8+ - ES10c
SF.EUICC.LPAe	The TOE implements LP Ae features as described in [SGP.22]. Part of this feature is support for additional secure protocol channels which are part of the services provided by the TOE. The SCP in scope are: - ES11 - ES9+ Supported TLS version is TLS v1.2 with supported cipher suites TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 The Local User Interface (LUi) is not implemented in the TOE.
SF.EUICC.IP Ae	The TOE implements IP Ae features as described in [SGP.32]. Part of this feature is support for additional secure protocol channels which are part of the services provided by the TOE. The SCP in scope are: - ES11 - ES9+ Supported TLS version is TLS v1.2 with supported cipher suites TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Table 31 eUICC Security Functions

9.2 Runtime Environment security functions

Security Functions (SF)	Description
SF.JC.FW	The TOE provides isolation of user spaces by means of a firewall.
SF.JC.RIP	The TOE provides features to guarantee information from different sources made unavailable after destruction. A list of type of data and feature is listed below:

Security Functions (SF)	Description
	• Objects: Garbage Collector • Transient data: Logical channels • Persistent data: Transaction mechanism • Packages/CAP files: Card Manager • Keys: Cryptographic containers
SF.JC.CRYPTO	The TOE provides a number of API which links to cryptographic support (key management, cryptographic operations, etc.) and PIN features. The cryptographic algorithms in supported but not in scope as a service are AES, T-DES, ECDH, ECDSA, EC KeyGen, SHA-256, HMAC. Nevertheless, these algorithms will provide support to SF.GP.SCP and SF.EUICC.SCP. Moreover, TOE provides SHA-256 (as required by [SGP.22]) for different purposes, such as KDF, HMAC or Hash generation.
SF.JC.ROLLBACK	The TOE provides features to provide atomic operation in the context of a transaction. For these operations, recovery of data is warranted with rollback and roll forward operations.
SF.GP.CM	The TOE implements GlobalPlatform functions natively. The implementation includes 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 functions natively. 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: • SCP80 • SCP81 (TLS_PSK_WITH_AES_128_CBC_SHA256) • SCP-SGP22 The SCP-SGP22 includes SCP03 and SCP03t

Table 32 Global Platform Security Functions

9.3 OS Update security functions

Security Functions (SF)	Description
SF.OSUPDATE	The TOE implements OS Update functionalities covering requirements as defined in [GPCS]. The implementation includes an application that provides functionalities to manage new OS images including: • OS image downloading • OS image activation

Table 33 OS Update Security Functions

9.4 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.

9.4.1 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.6/Mobile_network
SF.EUICC.SECDOM	FIA_UID.1/EXT, FIA_UAU.1/EXT, FIA_USB.1/EXT, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD, FIA_USB.1/MNO-SD, FIA_ATD.1/Base, FIA_API.1 FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FPT_FLS.1/Platform_services FCS_RNG.1, FPT_EMS.1/Base, FDP_SDI.1/Base, FDP_RIP.1/Base, FPT_FLS.1/Base, FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/Rules, FMT_MSA.1/CERT_KEYS, FMT_SMF.1/Base, FMT_SMR.1/Base, FMT_MSA.1/RAT, FMT_MSA.3/Base
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.6/SCP-SM and FCS_CKM.6/SCP-MNO
SF.EUICC.LPaE (LUI is not implemented in the TOE)	FIA_ATD.1/Base, FMT_MSA.1/CERT_KEYS, FMT_MSA.3/Base, FIA_UID.1/LPaE, FIA_UAU.1/LPaE, FIA_USB.1/LPaE, FIA_UAU.4/LPaE, FIA_ATD.1/LPaE, FDP_IFC.1/LPaE, FDP_IFF.1/LPaE, FTP_ITC.1/LPaE, FDP_ITC.2/LPaE, FPT_TDC.1/LPaE, FDP_UCT.1/LPaE, FDP_UIT.1/LPaE, FCS_CKM.1/LPaE, FCS_CKM.6/LPaE, FPT_EMS.1/LPaE, FDP_SDI.1/LPaE, FDP_RIP.1/LPaE, FMT_SMF.1/LPaE, FMT_SMR.1/LPaE
SF.EUICC.IPaE	FIA_ATD.1/Base, FMT_MSA.1/CERT_KEYS, FMT_MSA.3/Base, FIA_UID.1/IPaE, FIA_UAU.1/IPaE, FIA_USB.1/IPaE, FIA_UAU.4/IPaE, FIA_ATD.1/IPaE, FDP_IFC.1/IPaE, FDP_IFF.1/IPaE, FTP_ITC.1/IPaE, FDP_ITC.2/IPaE, FPT_TDC.1/IPaE, FDP_UCT.1/IPaE, FDP_UIT.1/IPaE, FCS_CKM.1/IPaE, FCS_CKM.6/IPaE, FPT_EMS.1/IPaE, FDP_SDI.1/IPaE, FDP_RIP.1/IPaE, FMT_SMF.1/IPaE, FMT_SMR.1/IPaE

Table 34 eUICC SFR Mapping Rationale

9.4.2 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
SF.JC.CRYPTO	FPR_UNO.1, FCS_RNG.1 and FPT_EMS.1/Base, FCS_COP.1/ECDH, FCS_COP.1/MD, FCS_COP.1/MAC_TDES, FCS_COP.1/MAC_AES,

Security Functions (SF)	SFR Mapping Rationale
	FCS_COP.1/SIG_ECC, FCS_COP.1/CIPH_TDES_CBC, FCS_COP.1/CIPH_AES_GCM, FCS_COP.1/CIPH_AES_CBC, FCS_COP.1/HMAC, FCS_CKM.1/SIG_ECC, FCS_CKM.1/ECDH, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.6/RE
SF.JC.ROLLBACK	FDP_RIP.1/ABORT, FPT_RCV.3/OS, FPT_RCV.4/OS, FAU_SAS.1
SF.GP.CM	FIA_AFL.1/GP, FAU_ARP.1, FDP_SDI.2/DATA, FPT_FLS.1/JC, FPT_TDC.1/JC, FIA_ATD.1/AID, FIA_UID.2/AID, FIA_USB.1/AID, FDP_ITC.2/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_UID.1/CM, FIA_UAU.1/GP, FIA_UAU.4/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FMT_SMF.1/CM, FMT_SMR.1/CM, FMT_MSA.1/CM, FMT_MSA.3/CM and FCO_NRO.2/CM, FDP_IFC.2/CM, FDP_IFF.1/CM, FDP_ITC.1/CM, FDP_UIT.1/CM
SF.GP.SCP	FDP_IFC.1/SCP, FDP_IFF.1/SCP, FDP_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.6/SCP-SM and FCS_CKM.6/SCP-MNO

Table 35 Global Platform SFR Mapping Rationale

9.4.3 OS Update SFRs coverage

Security Functions (SF)	Description
SF.OSUPDATE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FIA_ATD.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FMT_SMF.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC and FCS_COP.1/OS-UPDATE-VER, FPT_FLS.1/OS-UPDATE

Table 36 OS Update SFR Mapping Rationale